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

Audit Report

Department of Energy's Fiscal Year 2011 Consolidated Financial Statements

OAS-FS-12-02 November 2011

Department of Energy
Washington, DC 20585

November 15, 2011

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Report on the Department of Energy's Fiscal Year 2011 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 (Department) Fiscal Year (FY) 2011 Consolidated Financial Statements.

KPMG audited the consolidated balance sheets of the Department as of September 30, 2011 and 2010, 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 U.S. generally accepted accounting principles and has issued an unqualified opinion based on its audits and the reports of other auditors for the year ended September 30, 2011.

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 over financial reporting 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 oversight of cyber security reform efforts, issuing guidance, and the development of a cyber security management architecture framework to support the Department's mission-based 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 OIG 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 where KPMG did not comply with applicable auditing standards.

I would like to thank each of the Department elements for their courtesy and cooperation during the review.

Attachment

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

Audit Report: OAS-FS-12-02

http://www.cfo.doe.gov/cf12/2011parAFR.pdf

KPMG LLP
2001 M Street, NW
Washington, DC 20036-3389

INDEPENDENT AUDITORS' REPORT

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

We have audited the accompanying consolidated balance sheets of the United States Department of Energy (Department) as of September 30, 2011 and 2010, 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 (hereinafter referred to as "consolidated financial statements"). The objective of our audits was to express an opinion on the fair presentation of these consolidated financial statements. In connection with our fiscal year 2011 audit, we also considered the Department's internal control over financial reporting and tested the Department's compliance with certain provisions of applicable laws, regulations, contracts, and grant agreements that could have a direct and material effect on these consolidated financial statements.

As discussed in this report, a Power Marketing Administration of the Department, whose Department-related financial data is included in the accompanying consolidated financial statements, was audited by other auditors whose report has been furnished to us and was considered in forming our overall opinion on the Department's consolidated financial statements.

SUMMARY

As stated in our opinion on the consolidated financial statements, based upon our audits and the report of the other auditors, we concluded that the Department's consolidated financial statements as of and for the years ended September 30, 2011 and 2010, are presented fairly, in all material respects, in conformity with U.S. generally accepted accounting principles.

Our opinion emphasizes that: (1) the Department has loans and loan guarantees issued under the Federal Credit Reform Act of 1990 and that subsidy costs of the loans and loan guarantees include interest rate differentials, delinquencies, defaults, fees and other cash flow items; (2) the cost estimates supporting the Department's environmental remediation liabilities are based upon assumptions regarding funding and other future actions and decisions, many of which are beyond the Department's control; and (3) 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.

Our consideration of internal control over financial reporting resulted in identifying certain deficiencies related to unclassified network and information systems security, that we consider to be a significant deficiency, as defined in the Internal Control Over Financial Reporting section of this report.

We did not identify any deficiencies in internal control over financial reporting that we consider to be material weaknesses as defined in the Internal Control Over Financial Reporting section of this report.

The results of our tests of compliance with certain provisions of laws, regulations, contracts, and grant agreements disclosed no instances of noncompliance or other matters that are required to be reported herein

under *Government Auditing Standards* and Office of Management and Budget (OMB) Bulletin Number (No.) 07-04, *Audit Requirements for Federal Financial Statements*, as amended.

The following sections discuss our opinion on the Department's consolidated financial statements; our consideration of the Department's internal control over financial reporting; our tests of the Department's compliance with certain provisions of applicable laws, regulations, contracts, and grant agreements; and management's and our responsibilities.

OPINION ON THE FINANCIAL STATEMENTS

We have audited the accompanying consolidated balance sheets of the United States Department of Energy as of September 30, 2011 and 2010, and the related consolidated statements of net cost, changes in net position, and custodial activity, and the combined statements of budgetary resources for the years then ended.

We did not audit the financial statements of Bonneville Power Administration as of and for the years ended September 30, 2011 and 2010, whose Department-related financial data reflect total assets constituting 12.2 percent and 10.7 percent and total net costs constituting (0.6) percent and (0.2) percent, respectively, of the related consolidated totals. Those financial statements were audited by other auditors whose report has been furnished to us, and our opinion, insofar as it relates to the amounts included for Bonneville Power Administration, is based solely upon the report of the other auditors.

In our opinion, based on our audits and the report of the other auditors, 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, 2011 and 2010, and its net costs, changes in net position, budgetary resources, and custodial activity for the years then ended, in conformity with U.S. generally accepted accounting principles.

As discussed in Note 7 to the consolidated financial statements, the Department has total direct loans and loan guarantees, net, of $7.1 billion and $2.5 billion as of September 30, 2011 and 2010, respectively, which are issued under the Federal Credit Reform Act of 1990. Subsidy costs of the loan 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 remediation liabilities of $251 billion and $250 billion as of September 30, 2011 and 2010, 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 $19 billion and $15 billion as of September 30, 2011 and 2010, respectively.

The information in the Management's Discussion and Analysis, Required Supplementary Information, and Required Supplementary Stewardship Information sections is not a required part of the consolidated financial statements, but is supplementary information required by U.S. generally accepted accounting principles. We and the other auditors have applied certain limited procedures, which consisted principally of inquiries of management regarding the methods of measurement and presentation of this information. However, we did not audit this information and, accordingly, we express no opinion on it.

Our audits were conducted for the purpose of forming an opinion on the consolidated financial statements taken as a whole. The information in the Consolidating Schedules section of the Department's 2011 *Agency Financial Report* is presented for purposes of additional analysis of the consolidated financial statements rather than to present the financial position, net costs, changes in net position, budgetary resources, and custodial activity of the Department's components individually. The September 30, 2011 consolidating information has been subjected to the auditing procedures applied in the audit of the consolidated financial statements and, in our opinion, based upon our audits and the report of the other auditors, is fairly stated, in all material respects, in relation to the consolidated financial statements taken as a whole.

The information in the Message from the Secretary and Other Accompanying Information section of the Department's 2011 *Agency Financial Report* is presented for purposes of additional analysis and is not required as part of the consolidated financial statements. This information has not been subjected to auditing procedures and, accordingly, we express no opinion on it.

INTERNAL CONTROL OVER FINANCIAL REPORTING

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.

Our consideration of internal control over financial reporting was for the limited purpose described in the Responsibilities section of this report and was not designed to identify all deficiencies in internal control over financial reporting that might be deficiencies, significant deficiencies, or material weaknesses. This report also includes our consideration of the results of the other auditors' testing of internal control over financial reporting that are reported on separately by those auditors. However, this report, insofar as it relates to the results of the other auditors' testing, is based solely on the report of the other auditors.

In our fiscal year 2011 audit, we did not identify any deficiencies in internal control over financial reporting that we consider to be material weaknesses, as defined above. However, we identified certain deficiencies in internal control over financial reporting related to unclassified network and information systems security, as described below and in more detail in Exhibit I, that we consider to be a significant deficiency in internal control over financial reporting. 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.

- *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.

Exhibit II presents the status of the prior year significant deficiency.

We noted certain additional matters involving internal control over financial reporting and internal control over financial management systems that we will report to management in separate letters.

COMPLIANCE AND OTHER MATTERS

The results of our tests of compliance described in the Responsibilities section of this report, exclusive of those referred to in the *Federal Financial Management Improvement Act of 1996* (FFMIA), disclosed no instances of noncompliance or other matters that are required to be reported herein under *Government Auditing Standards* or OMB Bulletin No. 07-04, as amended. This report also includes our consideration of the results of the other auditors' testing of compliance and other matters that are reported on separately by the other auditors. However, this report, insofar as it relates to the results of the other auditors' testing, is based solely on the report of the other auditors.

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.

RESPONSIBILITIES

Management's Responsibilities. Management is responsible for the consolidated financial statements; establishing and maintaining effective internal control; and complying with laws, regulations, contracts, and grant agreements applicable to the Department.

Auditors' Responsibilities. Our responsibility is to express an opinion on the fiscal year 2011 and 2010 consolidated financial statements of the Department based on our audits and the report of the other auditors. 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 OMB Bulletin No. 07-04, as amended. Those standards and OMB Bulletin No. 07-04, as amended, require that we plan and perform the audits to obtain reasonable assurance about whether the consolidated financial statements are free of material misstatement. An audit includes consideration of internal control over financial reporting as a basis for designing audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the Department's internal control over financial reporting. Accordingly, we express no such opinion.

An audit also includes:

- Examining, on a test basis, evidence supporting the amounts and disclosures in the consolidated financial statements;
- Assessing the accounting principles used and significant estimates made by management; and

- Evaluating the overall consolidated financial statement presentation.

We believe that our audits and the report of the other auditors provide a reasonable basis for our opinion.

In planning and performing our fiscal year 2011 audit, we considered the Department's internal control over financial reporting by obtaining an understanding of the Department's internal control, determining whether internal controls had been placed in operation, assessing control risk, and performing tests of controls as a basis for designing our auditing procedures 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 over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the Department's internal control over financial reporting. Furthermore, we did not test all controls relevant to operating objectives as broadly defined by the *Federal Managers' Financial Integrity Act of 1982*.

As part of obtaining reasonable assurance about whether the Department's fiscal year 2011 consolidated financial statements are free of material misstatement, we performed tests of the Department's 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 the consolidated financial statement amounts, and certain provisions of other laws and regulations specified in OMB Bulletin No. 07-04, as amended, including the provisions referred to in Section 803(a) of FFMIA. We limited our tests of compliance to the provisions described in the preceding sentence, and we did not test compliance with all laws, regulations, contracts, and grant agreements applicable to the Department. However, providing an opinion on compliance with laws, regulations, contracts, and grant agreements was not an objective of our audit and, accordingly, we do not express such an opinion.

The Department's response to the findings identified in our audit is presented in Exhibit I. We did not audit the Department's response and, accordingly, we express no opinion on it.

This report is intended solely for the information and use of the Department's management, the Department's Office of Inspector General, OMB, the U.S. Government Accountability Office, and the U.S. Congress and is not intended to be and should not be used by anyone other than these specified parties.

KPMG LLP

November 14, 2011

Unclassified Network and Information Systems Security

The United States Department of Energy (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, these corrective actions had not been completed. The frequency of network security weaknesses reported by KPMG LLP has increased when compared to the prior year weaknesses, although the severity of these weaknesses remains consistent with prior year weaknesses. The Department recognizes the need to enhance its unclassified cyber security program and has categorized unclassified cyber security as a leadership challenge in its *Federal Managers' Financial Integrity Act* assurance statement for fiscal year 2011. Improvements are still needed in the areas of system and application access and related access privileges, password management, configuration management, and restriction of network services.

Our fiscal year 2011 audit disclosed information system security deficiencies similar in type and risk level to our findings in prior years. Specifically, we noted weaknesses within layered security controls for network servers, 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 found weak account management and monitoring controls for approval, provisioning, and termination of administrative and user accounts that may increase the risk of malicious or unauthorized access to systems and data.

In the area of configuration and vulnerability management, we identified deficiencies in the patch management process for timely and secure installation of critical software patches, with numerous instances in which security patches had not been applied to correct known vulnerabilities more than three months after the patches became available. We also noted numerous weaknesses in web application integrity as a result of design flaws in those applications. We identified web applications that did not properly validate input data or utilize safe database queries, 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 cyber security weaknesses were corrected immediately after we identified and reported them to site management, deficiencies in the process for identifying, monitoring, and remediating such deficiencies have continued from prior years. We also identified inconsistent risk management practices at several sites and noted that site management had not established a risk acceptance process to fully document acceptance of risk. We further noted that multiple sites were continuing to develop and implement the Department's revised risk management framework to address these weaknesses. However, these risk management enhancements were incomplete at the time of our testing.

The Department's Office of Inspector General (OIG) reported on these deficiencies in its evaluation report on *The Department's Unclassified Cyber Security Program - 2011*, dated October 20, 2011. The OIG noted that identified weaknesses occurred, in part, because Departmental entities had not ensured that cyber security requirements included all necessary elements and were properly implemented. The OIG reported that program elements did not always utilize effective performance monitoring activities to ensure that appropriate security controls were in place. The OIG also reported deficiencies in configuration management programs at several sites where, even when policies and procedures were established, implementation of those policies and procedures were sometimes inconsistent. At other sites,

policies were not aligned with Federal requirements related to access controls and vulnerability and configuration management.

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 fiscal year 2011, the Department had taken steps to enhance its unclassified cyber security program, including oversight of continuing cyber security reform efforts from the Computer Security Governance Council at the Under Secretary level; issuance of additional guidance related to continuous monitoring and assessment of the risk management process in the new cyber directive, DOE Order 205.1B, *Department of Energy Cyber Security Program;* and development of a cyber security management architecture framework to support the Department's mission-based risk management approach.

Recommendation:

While some progress has been made, continued efforts are needed to effectively manage the evolving nature of cyber security threats, including strengthening the management review process and monitoring of field sites to ensure the adequacy of cyber security 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 ensure that systems are properly configured, implemented and updated throughout the lifetime of those systems.

Therefore, we recommend that the Under Secretary for Nuclear Security, Under Secretary of Energy, and Under Secretary for Science, in coordination with the Department and National Nuclear Security Administration Chief Information Officers, fully implement policies and procedures to ensure that the Federal cyber security standards are met, 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 ensure the effectiveness of sites' cyber security program implementation. Detailed recommendations to address the issues discussed above have been separately reported to the cognizant management officials.

Management's Response:

During FY 2011, the Office of the Chief Information Officer (OCIO) made good progress towards institutionalizing a Departmental risk-based approach to cybersecurity, including the issuance of DOE Order 205.1B, which codifies the governance structure and risk-managed implementation and measurement. In the Order, the responsibility for defining the risk profile and implementation requirements for Departmental operating units falls to the Under Secretary-level organizations, which are grouped for the sake of cybersecurity as Senior DOE Management (SDM). The SDM organizations are also responsible, through the deployment of contractor assurance systems (CAS), for graded oversight of their operating units' cybersecurity programs based on risk and past performance. Through these mechanisms, the operating unit implementation of Federal cybersecurity standards and mission-related risk management are monitored and assessed. In the few months since the Order was issued, work has been completed within the SDM organizations to prepare the Risk Management Approach (RMA) Implementation Plans that will bring both common policies and procedures to the operating units but also initiate oversight of cybersecurity program performance. The SDM level programs are still maturing; when fully documented and deployed, however, the CAS and oversight by local Federal managers will

allow for closer monitoring of risk-based cybersecurity, better assessment of its effectiveness, and prompt remediation of program performance issues.

Energy Information Technology Services (EITS), operated by the OCIO, is included in the OCIO SDM RMA Implementation Plan.

Throughout FY 2012, the OCIO will continue to refine the policy that defines the Departmental cybersecurity program, develop and maintain the Departmental risk management approach, and will begin to issue supplemental implementing guidance and requested assistance, as required by DOE O 205.1B, to the SDMs.

Fiscal Year 2010 Audit Findings (with parenthetical disclosure of year first reported)	**Status at September 30, 2011**
Unclassified Information Systems Security – Considered a Significant Deficiency (1999)	Not fully implemented – Unclassified network and information systems security issues continue to be reported in Exhibit I as a significant deficiency.

IG Report No. OAS-FS-12-02

CUSTOMER RESPONSE FORM

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

1. What additional background information about the selection, scheduling, scope, or procedures of the inspection would have been helpful to the reader in understanding this report?

2. What additional information related to findings and recommendations could have been included in the report to assist management in implementing corrective actions?

3. What format, stylistic, or organizational changes might have made this report's overall message more clear to the reader?

4. What additional actions could the Office of Inspector General have taken on the issues discussed in this report which would have been helpful?

5. Please include your name and telephone number so that we may contact you should we have any questions about your comments.

Name _____ Date _____

Telephone _____ Organization _____

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

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

ATTN: Customer Relations

If you wish to discuss this report or your comments with a staff member of the Office of Inspector General, please contact Felicia Jones 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.