Department of Energy
Washington, DC 20585

November 12, 2010

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Report on the Department of Energy's Fiscal Year 2010 Consolidated Financial Statements

This is to inform you that the audit of the Department of Energy's (Department) Fiscal Year (FY) 2010 Consolidated Financial Statements has resulted in an unqualified audit opinion. Pursuant to requirements established by the Government Management Reform Act of 1994, the Office of Inspector General (OIG) engaged the independent public accounting firm of KPMG LLP (KPMG) to perform the audit. KPMG was responsible for expressing an opinion on the Department's consolidated financial statements based on its audits and the reports of other auditors for the year ended September 30, 2010.

KPMG concluded that the consolidated financial statements present fairly, in all material respects, the financial position of the Department and its net costs, changes in net position, budgetary resources and custodial activity in conformity with U.S. generally accepted accounting principles.

As part of the 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 the following issue related to unclassified network and information systems security that, while not classified as a material weakness, was considered to be a significant deficiency:

- Unclassified Network and Information Systems Security: While the Department has made progress in addressing previously identified cyber security weaknesses, network vulnerabilities and weaknesses in access and other security controls in the Department's unclassified computer information systems continue to exist. Management recognized the critical importance of protecting its corporate financial systems and data and was taking steps to improve the management and implementation of its cyber security program.

The audit disclosed no instances of noncompliance that are required to be reported under applicable audit standards and requirements. With regard to the specific findings associated with the significant deficiency, the Department concurred and agreed to take corrective actions.

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
Acting Under Secretary of Energy
Under Secretary for Science
Chief of Staff
Chief Information Officer
Chief Financial Officer

Audit Report: OAS-FS-11-01

http://www.cfo.doe.gov/cf12/2010parAFR.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, 2010 and 2009, and the related consolidated statements of net cost, changes in net position, and custodial activity, and the combined statements of budgetary resources (hereinafter referred to as "consolidated financial statements") for the years then ended. 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 2010 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, 2010 and 2009, are presented fairly, in all material respects, in conformity with U.S. generally accepted accounting principles.

Our opinion emphasizes that: (1) 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 (2) 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 under *Government Auditing Standards*, issued by the Comptroller General of the United States, and Office of Management and Budget (OMB) Bulletin 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, 2010 and 2009, 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, 2010 and 2009, whose Department-related financial data reflect total assets constituting 10.7 percent and 10.7 percent and total net costs constituting (0.2) percent and (0.1) percent, respectively, of the related consolidated totals. Those financial statements were audited by the 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, 2010 and 2009, 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 15 to the consolidated financial statements, the cost estimates supporting the Department's environmental remediation liabilities of $250 billion and $268 billion as of September 30, 2010 and 2009, 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 $15 billion and $13 billion as of September 30, 2010 and 2009, 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 2010 *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, 2010 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 the Other Accompanying Information section of the Department's 2010 *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 Department'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 2010 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 described 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 prior year significant deficiencies.

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 2010 and 2009 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 2010 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 2010 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 12, 2010

Independent Auditors' Report
Exhibit I – Significant Deficiency

Unclassified Network and Information Systems Security

The Department 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, we continued to identify similar weaknesses in security controls at the sites we reviewed in fiscal year 2010. 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 2010. 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 2010 audit disclosed information system security deficiencies consistent with 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 blank or easily guessed administrator or user passwords on network systems that could permit unauthorized access to those systems and their data. We also found weak access controls for shared directories and files, in which unauthorized users could potentially gain access to sensitive data, including personally identifiable information, or modify configuration settings.

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 identified instances where sites had not correctly configured their vulnerability scanning software to ensure known vulnerabilities were identified and remediated in a timely manner, or had not fully implemented an effective vulnerability and patch management program as a result of having insufficient vulnerability scanning licenses to scan all systems.

While many of these cyber security deficiencies were corrected immediately after we identified and reported them to site management, weaknesses in the process for identifying, monitoring, and remediating such deficiencies have continued from prior years. In several instances, the sites had not fully implemented procedures designed to ensure that minimum cyber security requirements were met. Furthermore, even when policies and procedures were established, implementation of those policies and procedures were sometimes inconsistent and sites had not always validated, through testing or other means, that the procedures were operating effectively.

The Department's Office of Inspector General (OIG) reported on these deficiencies in its evaluation report on *The Department's Unclassified Cyber Security Program - 2010*, dated October 2010. The OIG noted that identified weaknesses occurred, in part, because Departmental elements had not always ensured that cyber security requirements were effectively implemented. Consistent with prior year findings, the OIG reported that the National Nuclear Security Administration (NNSA) had begun, but not fully implemented, a program for management oversight and periodic evaluation of the cyber security practices of its Federal sites offices and associated field sites. The OIG also identified deficiencies in configuration management processes at several sites in which, contrary to the Department's policies and procedures, systems were

placed into operation prior to completing required system security plans or following incomplete testing of security controls.

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 2010, the Department has taken positive steps to enhance its unclassified cyber security program, including establishing a Computer Security Governance Council at the Under Secretary level to oversee its cyber security reform efforts, refining cyber security policies and procedures, and initiating the implementation of an automated tool to aid in cyber security and performance reporting.

Recommendation:

While some progress has been made, continued efforts are needed to strengthen the management review process to include better monitoring of field sites to ensure the adequacy of cyber security program performance, fully implement government-wide security configuration standards that establish minimum baseline security controls, and employ the use of automated tools compatible with the baseline standards in the resolution of the vulnerabilities and control weaknesses described above.

Therefore, we recommend that the Department's Chief Information Officer (CIO), in conjunction with NNSA and other cognizant program officials, 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 program offices and the Office of the CIO (OCIO).

Management's Response:

The Department has taken numerous steps to improve the management and implementation of cyber security in this past fiscal year. These steps include the formation of the Information Management Governance Council, which is comprised of the Department's most senior leadership, and the Department's transition to a mission centric, risk-based approach for the management of the Department's Cyber Security Program. The Department recognizes the critical importance of protecting its corporate financial systems and data, and is committed to improving its cyber security posture by taking proactive steps to assess new threats and maintain secure system configurations. We are revising our cyber security strategic plan, architecture framework, and training and awareness programs. The Department is also assessing its overall incident management capabilities to improve coordination and collaboration.

However, without additional identifying data with which to connect the IG's cyber security findings to specific financial systems and deficiencies in financial reporting, it is difficult to correlate these deficiencies. Such correlation would enable the CIO to determine whether they materially or even consequentially impact the Department's financial statements and the integrity of its financial reporting.

We share the IG's goal to improve our cyber security programs and to better protect the missions of DOE. To better facilitate the process for achieving this goal, we request that the IG share additional details with the CIO in order to facilitate timely improvement and enhancement of our cyber security posture.

Auditor Comments:

As noted in management's response, the Department had taken steps to improve management and implementation of its cyber security program over the past year. However, we take exception to management's comments that the OIG did not provide adequate information to the Department to support the vulnerabilities identified above. Specifically, as with prior years, we provided each of the sites reviewed with extensive information regarding identified weaknesses. In addition, numerous discussions were held with Department and contractor officials to help understand the risk management process, review the vulnerabilities identified, and determine potential mitigating controls. Furthermore, each of the findings issued were provided to Headquarters and field site officials, including the respective Under Secretary organizations, OCIO and NNSA. Going forward, we will continue to work with management to improve the Department's cyber security program and better protect the missions of the Department.

Independent Auditors' Report
Exhibit II – Status of Prior Year Audit Findings

Fiscal Year 2009 Audit Findings (with parenthetical disclosure of year first reported)	**Status at September 30, 2010**
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.
Accounting of Property, Plant, and Equipment – Considered a Significant Deficiency (2009)	Significant actions implemented – No longer considered a significant deficiency.