U.S. Department of Energy

Office of Inspector General

Office of Audits and Inspections

AUDIT REPORT

Department of Energy's Fiscal Year 2014 Consolidated Financial Statements

OAS-FS-15-01

November 2014

Department of Energy
Washington, DC 20585

November 17, 2014

MEMORANDUM FOR THE SECRETARY

FROM: Gregory H. Friedman
Inspector General

SUBJECT: INFORMATION: Audit Report on "Department of Energy's Fiscal Year 2014 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 2014 Consolidated Financial Statements.

KPMG audited the consolidated financial statements of the Department as of September 30, 2014 and 2013, 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, 2014 and 2013.

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 improve its unclassified cybersecurity program, including formalizing and approving a framework to support mission enhancement, operational excellence and risk management, and enhancing a continuous monitoring program that, when fully implemented, should facilitate near real-time situational awareness and appropriate cost-effective risk based decisions.

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
Deputy Under Secretary for Science and Energy
Deputy Under Secretary for Management and Performance
Chief of Staff
Deputy Chief Financial Officer

Audit Report: OAS-FS-15-01

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

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

Attachment

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, 2014 and 2013, 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, 2014 and 2013, 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 $16 billion and $15 billion as of September 30, 2014 and 2013, 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. Our opinion is not modified with respect to this matter.

As discussed in Note 15 to the consolidated financial statements, the cost estimates supporting the Department's environmental cleanup and disposal liabilities of $300 billion and $280 billion as of September 30, 2014 and 2013, respectively, are based upon assumptions regarding funding and other future actions and decisions, many of which are beyond the Department's control. Our opinion is not modified with respect to this matter.

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 $23 billion and $21 billion as of September 30, 2014 and 2013, respectively. Our opinion is not modified with respect to this matter.

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, the Message from the Secretary, the Message from the Chief Financial Officer, and Other Information section of the Department's 2014 *Agency Financial Report* are presented for purposes of additional analysis and are 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, the Message from the Chief Financial Officer, and Other Information section of the Department's 2014 *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 as of and for the year ended September 30, 2014, 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, 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 protect networks and information systems against unauthorized access and implement an adequate performance monitoring and risk management program 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

November 14, 2014

Independent Auditors' Report
Exhibit I – Significant Deficiency
Unclassified Network and Information Systems Security

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 Independent Enterprise Assessments, reviewed in prior years. However, at the time of our testing, corrective actions had not been fully completed.

The severity of network security weaknesses reported by KPMG remains consistent with prior year weaknesses. The Department recognizes the need to enhance its unclassified cybersecurity program and continues to implement corrective action plans as reported in its *Federal Managers' Financial Integrity Act* assurance statement for fiscal year (FY) 2014. Improvements are still needed in the areas of system and application access controls, configuration management, security patch management and system integrity.

Our FY 2014 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. The affected systems included servers providing core network services, workstations used by financial application users and system administrators with privileged levels of access to financial applications and other network systems, and web applications supporting business, human resources and general support 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 deficiencies in configuration and vulnerability management on network server and desktop systems. 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, and at several sites, more than 90 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 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 certain weaknesses were corrected immediately after we identified and reported them to site management, deficiencies in cybersecurity processes and procedures have continued from prior years. Numerous network and information security weaknesses previously identified in FY 2010 and 2011 at two sites had not been remediated at the time of our review. These weaknesses, if left uncorrected, could adversely affect the Department's ability to identify, assess and mitigate new and existing threats and risks to its information systems and data.

We noted that numerous sites had not fully implemented cybersecurity processes that could have prevented many of the weaknesses identified during our testing. At multiple locations, network and information system security processes and procedures had been implemented but were not operating effectively or being followed in accordance with site-defined policies. Specifically, these processes and procedures, including security testing and validation, standard baseline configurations, secure software coding, automated security updates, and continuous monitoring were not fully implemented to identify, monitor and remediate system vulnerabilities and to prevent unauthorized access by internal and external sources.

The Department's programs and sites are continuing to transition from a traditional compliance-based cybersecurity process to one that supports the National Institute of Standards and Technology's Risk Management Framework and continuous system authorizations. Numerous locations we reviewed were continuing to develop and implement site-level Implementation Plans in accordance with the Department's Risk Management Approach to manage information system-related security risks and make risk-based decisions. Although certain sites had developed the process of assessing risk and determining the approach to risk management, the process did not include all cybersecurity elements and had not been fully implemented in the sites' unclassified cybersecurity programs. 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 of Energy's Unclassified Cybersecurity Program - 2014*, dated October 2014. The OIG noted that the identified weaknesses occurred, in part, because the Department's programs and sites had not ensured that cybersecurity policies and procedures were developed and properly implemented. The OIG reported that the Department's performance monitoring and risk management programs were not completely effective. The OIG also noted that continued network and information system security deficiencies could render the Department unable to gain or retain assurance that its systems and data are operated and maintained within acceptable levels of risk.

Although certain controls had been implemented at the sites we reviewed to mitigate the risk associated with these security weaknesses, these controls may not protect against many attacks, including publicly available exploits and custom attacks with no known signatures. 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 2014, the Department had taken steps to improve its unclassified cybersecurity program. The Department's Cyber Council formalized and approved its Information Management Governance Framework to support mission enhancement, operational excellence and risk management across the Department. Additionally, the National Nuclear Security Administration continued to enhance its Enterprise Continuous Monitoring Program that, when fully implemented, should facilitate near real-time situational awareness and appropriate cost-effective risk-based decisions at its sites, including Headquarters.

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 security testing and validation 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, Acting Under Secretary for Science and Energy, and Acting Under Secretary for Management and Performance, in coordination with the Department and National Nuclear Security Administration Chief Information Officers, correct, through the implementation of appropriate controls, the weaknesses identified during our review; ensure that networks and information systems are adequately protected against unauthorized access to a level of risk commensurate with the criticality of the systems and the sensitivity of the information within them; and ensure that an adequate performance monitoring and risk management program is implemented to improve the effectiveness of the Department's unclassified 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's Office of Chief Information Officer (OCIO) and Office of the Chief Financial Officer (OCFO) appreciate the opportunity to comment on the Significant Deficiency Report. The OCIO and the OCFO acknowledge the FY 2014 findings and note that these findings represent a 36% reduction in the number of findings from FY 2013. The auditors recognized in their report that there are mitigating controls in place to ensure the integrity of the financial systems and data. While the Department will address the findings and continue to improve and adhere to security control processes and procedures, we believe that the Department's financial data and systems are adequately protected.

As noted in this report, the Department has implemented corrective actions to address many of the identified findings at the sites where security controls were reviewed by the OIG and the Department's Office of Independent Enterprise Assessments in prior years. The OCIO acknowledges that remediation of some of these findings is not yet complete and recognizes the need to continue efforts to enhance unclassified cybersecurity programs across the Department and implement corrective action plans as reported in its *Federal Managers' Financial Integrity Act* assurance statement for FY 2014.

The Department continues its commitment to the protection of its information and information systems through strong comprehensive cybersecurity and privacy programs. The Department will take appropriate follow-up action on specific findings, as well as continue to work in the most effective way to improve the Department's overall cybersecurity posture. The following efforts support the continued improvement of the Department's risk-managed cybersecurity program at the enterprise and local levels.

- **Update of DOE Order 205.1B, *Department of Energy Cyber Security Program:*** The Department is updating DOE O 205.1B, which codifies a federated risk-based approach to cybersecurity planning, to align with recently released Federal laws, regulations, and guidelines. The Order will be updated to address application access control, configuration management, security patch management/vulnerability management, system integrity, and to codify authorities and responsibilities related to the documentation, implementation, and oversight of cybersecurity

activities across the Department. The new Order will address Federal requirements and will be consistent with National Institute of Standards and Technology (NIST) and Committee on National Security Systems (CNSS) direction and guidance. DOE will utilize this policy to model daily and long-term activities surrounding cybersecurity processes and controls, including access control, configuration management, vulnerability management, and system integrity as identified in this report.

- **Plans of Action and Milestones (POA&M):** The DOE OCIO has reviewed the weaknesses noted in this report and will confirm that they are recorded and tracked as POA&Ms. Each DOE program provides the estimated completion dates and corrective actions through quarterly POA&M reporting to the OCIO. The OCIO will enhance its capabilities to assess program POA&M reports for completeness and accuracy and initiate processes to validate POA&M information. The OCIO is leveraging its Enterprise Cyber Governance System (ECGS) to streamline POA&M tracking and reporting and provide a centralized repository for cybersecurity weakness remediation activities. This combined approach will assist the Program Offices in refining their processes for managing remediation activities, assessing weaknesses across the program, and prioritizing actions.

- **Information Management Governance Framework.** The Secretary's Cyber Council, which was launched in 2013, approved a new Information Management governance framework, developed in collaboration with program offices, staff offices, national labs, and other DOE sites. The Information Management Governance Board (IMGB) serves as the principal forum for coordinating information management and cybersecurity activities and issues across the Department. Issues concerning the strengthening of cybersecurity programs will be part of the agenda for this group.

- **Vulnerability Management and Continuous Monitoring.** DOE O 205.1B requires organizations to implement a risk-based approach to cybersecurity within their programs and systems. Organizations are required to incorporate continuous monitoring and vulnerability assessment and remediation in their documented programs to support informed risk management decisions, as well as to implement consistent patch management as recommended in NIST Special Publication 800-40. Organizations are further supported by programs such as Information Security Continuous Monitoring, which includes the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program. In 2013, DOE signed a Memorandum of Agreement with DHS to deploy CDM capability, including participation in "buying groups," and procurement authority to use DHS-administered contracts.

- **JC3**. The capabilities of the Joint Cybersecurity Coordination Center (JC3) continue to develop in support of DOE's efforts to address identified weaknesses, enhance its overall protective posture, and coordinate and strengthen incident response capabilities. The DOE follows all US-CERT and ICS-CERT reporting guidelines for computer security incidents and utilizes the US-CERT Incident Notification System. The JC3 is the primary interface with US-CERT and collects and delivers all incident notifications, alerts, and reports within US-CERT reporting guidelines. All incidents reported in FY 2014 have been resolved or remediated.

- **Strategy to Identify Significantly Vulnerable Systems.** An OCIO task force is developing an enterprise-wide strategy and framework for identifying and reporting the status of significantly vulnerable systems to DOE senior leadership. The framework will provide earlier indicators and recommendations from system owners, the Privacy Office, and DOE leadership concerning the operational status of significantly vulnerable systems. The strategy assumes that prompt identification of these assets enables leadership to quickly expend resources, as needed, to mitigate weaknesses and restore or enhance the cybersecurity posture of DOE enterprise networks.

- **IT Audit Working Group.** The OCFO will continue to work with the Program Offices and labs in FY 2015 to address improvements in information technology processes related to financial management and controls. In addition, the IT Audit Working Group was instrumental in closing numerous prior-year findings in FY 2014 and will be focused in FY 2015 on audit preparation, strengthening technical reviews of audit progress, and improving management responses to audit findings.

Auditor Comments

Management's comments are responsive to our recommendations. Management's planned corrective actions should, if fully implemented, help to further improve the Department's cybersecurity posture. Although we identified and tested compensating controls during our IT procedures that served to mitigate the potential impact of the security weaknesses on the integrity of data in the Department's financial applications, our audit is not for the purpose of expressing an opinion or providing assurance on the effectiveness of the Department’s internal controls, and accordingly, we express no such opinion or assurance on whether the controls ensure the integrity of the financial systems and data.

FEEDBACK

The Office of Inspector General has a continuing interest in improving the usefulness of its products. We aim to make our reports as responsive as possible and ask you to consider sharing your thoughts with us.

Please send your comments, suggestions and feedback to OIGReports@hq.doe.gov and include your name, contact information and the report number. Comments may also be mailed to:

Office of Inspector General (IG-12)
Department of Energy
Washington, DC 20585

If you want to discuss this report or your comments with a member of the Office of Inspector General staff, please contact our office at (202) 253-2162.