UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Washington, DC 20415

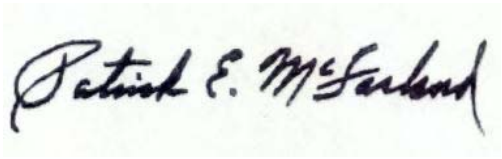
Office of the
Inspector General

November 13, 2015

Report No. 4A-CF-00-15-027

MEMORANDUM FOR BETH F. COBERT
Acting Director

FROM: PATRICK E. McFARLAND
Inspector General



SUBJECT: Audit of the Office of Personnel Management's Fiscal Year 2015 Consolidated Financial Statements

This memorandum transmits KPMG LLP's (KPMG) report on its financial statement audit of the Office of Personnel Management's (OPM) Fiscal Year 2015 Consolidated Financial Statements and the results of the Office of the Inspector General's (OIG) oversight of the audit and review of that report. OPM's consolidated financial statements include the Retirement Program, Health Benefits Program, Life Insurance Program, Revolving Fund Programs (RF) and Salaries & Expenses funds (S&E).

Audit Reports on Financial Statements, Internal Controls and Compliance with Laws and Regulations

The Chief Financial Officers (CFO) Act of 1990 (P.L. 101-576) requires OPM's Inspector General or an independent external auditor, as determined by the Inspector General, to audit the agency's financial statements in accordance with *Government Auditing Standards* (GAS) issued by the Comptroller General of the United States. We contracted with the independent certified public accounting firm KPMG to audit OPM's consolidated financial statements as of September 30, 2015 and for the fiscal year then ended. The contract requires that the audit be performed in accordance with generally accepted government auditing standards and the Office of Management and Budget (OMB) Bulletin No. 15-02, *Audit Requirements for Federal Financial Statements*.

KPMG's audit report for Fiscal Year 2015 includes: (1) opinions on the consolidated financial statements and the individual statements for the three benefit programs, (2) a report on internal controls, and (3) a report on compliance with laws and regulations. In its audit of OPM, KPMG found:

- The consolidated financial statements were fairly presented, in all material respects, in conformity with U.S. generally accepted accounting principles.

- KPMG's report identified one material weakness in the internal controls:

    - Information Systems Control Environment

  A material weakness is a deficiency, or 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.

- KPMG's report identified one significant deficiency:

    - Entity Level Controls Over Financial Management

  A significant deficiency is a deficiency, or 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.

- KPMG's report identified instances of non-compliance with the Federal Financial Management Improvement Act of 1996 (FFMIA), as described in the material weakness, in which OPM's financial management systems did not substantially comply with the Federal financial management systems requirements. The results of KPMG's tests of FFMIA disclosed no instances in which OPM's financial management systems did not substantially comply with applicable Federal accounting standards and the United States Government Standard General Ledger at the transaction level.

OIG Evaluation of KPMG's Audit Performance

In connection with the audit contract, we reviewed KPMG's report and related documentation and made inquiries of its representatives regarding the audit. To fulfill our audit responsibilities under the CFO Act for ensuring the quality of the audit work performed, we conducted a review of KPMG's audit of OPM's Fiscal Year 2015 Consolidated Financial Statements in accordance with GAS. Specifically, we:

- provided oversight, technical advice, and liaison to KPMG auditors;

- ensured that audits and audit reports were completed timely and in accordance with the requirements of Generally Accepted Government Auditing Standards (GAGAS), OMB Bulletin 15-02, and other applicable professional auditing standards;

- documented oversight activities and monitored audit status;

- reviewed responses to audit reports and reported significant disagreements to the audit follow-up official per OMB Circular No. A-50, Audit Follow-up;

- coordinated issuance of the audit report; and,

- performed other procedures we deemed necessary.

Our review, as differentiated from an audit in accordance with GAGAS, was not intended to enable us to express, and we do not express, opinions on OPM's financial statements or internal controls or on whether OPM's financial management systems substantially complied with the Federal Financial Management Improvement Act of 1996 or conclusions on compliance with laws and regulations. KPMG is responsible for the attached auditor's report dated November 12, 2015, and the conclusions expressed in the report. However, our review disclosed no instances where KPMG did not comply, in all material respects, with the generally accepted GAS.

In accordance with the OMB Circular A-50 and Public Law 103-355, all audit findings must be resolved within six months of the date of this report. The OMB Circular also requires that agency management officials provide a timely response to the final audit report indicating whether they agree or disagree with the audit findings and recommendations. When management is in agreement, the response should include planned corrective actions and target dates for achieving them. If management disagrees, the response must include the basis in fact, law or regulation for the disagreement.

To help ensure that the timeliness requirement for resolution is achieved, we ask that the CFO coordinate with the OPM audit follow-up office, Internal Oversight and Compliance (IOC), to provide their initial responses to us within 60 days from the date of this memorandum. IOC should be copied on all final report responses. Subsequent resolution activity for all audit findings should also be coordinated with IOC. The CFO should provide periodic reports through IOC to us, no less frequently than each March and September, detailing the status of corrective actions, including documentation to support this activity, until all findings have been resolved.

In closing, we would like to thank OPM's financial management staff for their professionalism during KPMG's audit and our oversight of the financial statement audit this year.

If you have any questions about KPMG's audit or our oversight, please contact me at 606-1200, or you may have a member of your staff contact Michael R. Esser, Assistant Inspector General for Audits, at 606-2143.

cc: Dennis D. Coleman
Chief Financial Officer

Daniel K. Marella
Deputy Chief Financial Officer

Donna K. Seymour
Chief Information Officer

Janet L. Barnes
Director, Internal Oversight and Compliance

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

Independent Auditors' Report

Director and Inspector General
United States Office of Personnel Management:

Report on the Financial Statements

We have audited the accompanying consolidated financial statements of the United States (U.S.) Office of Personnel Management (OPM), which comprise the consolidated balance sheets as of September 30, 2015 and 2014, and the related consolidated statements of net cost and changes in net position, and combined statements of budgetary resources for the years then ended, and the related notes to the consolidated financial statements (hereinafter referred to as "consolidated financial statements"). Additionally, we have audited the individual balance sheets of the Retirement, Health Benefits, and Life Insurance Programs (hereinafter referred to as the "Programs") as of September 30, 2015 and 2014, and the related individual statements of net cost, changes in net position, and budgetary resources for the years then ended (hereinafter referred to as the Programs' "individual financial statements").

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these consolidated financial statements and these Programs' individual 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 and the Programs' individual 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 and on the Programs' individual 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. 15-02, *Audit Requirements for Federal Financial Statements*. Those standards and OMB Bulletin No. 15-02 require that we plan and perform the audit to obtain reasonable assurance about whether the consolidated financial statements and the Programs' individual 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 and Programs' individual financial statements. The procedures selected depend on the auditors' judgment, including the assessment of the risks of material misstatement of the consolidated financial statements and Programs' individual 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 and Programs' individual 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 and the Programs' individual financial statements.

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

Opinions 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 Office of Personnel Management of September 30, 2015 and 2014, and its net costs, changes in net position, and budgetary resources for the years then ended in accordance with U.S. generally accepted accounting principles.

In our opinion, the Programs' individual financial statements referred to above present fairly, in all material respects, the financial position of each of the Programs as of September 30, 2015 and 2014, and their net costs, changes in net position, and budgetary resources for the years then ended in accordance with U.S. generally accepted accounting principles.

Other Matters

Management has elected to reference to information on websites or other forms of interactive data outside the *Agency Financial Report* to provide additional information for the users of its financial statements. Such information is not a required part of the basic consolidated financial statements or supplementary information required by the Federal Accounting Standards Advisory Board. The information on these websites or the other interactive data has not been subjected to any of our auditing procedures, and accordingly we do not express an opinion or provide any assurance on it.

Required Supplementary Information

U.S. generally accepted accounting principles require that the information in the Management's Discussion and Analysis and Required Supplementary Information sections be presented to supplement the basic consolidated financial statements and the Programs' individual financial statements. Such information, although not a part of the basic consolidated financial statements and the Programs' individual 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 and the Programs' individual 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 the Programs' individual financial statements, and other knowledge we obtained during our audits of the basic consolidated financial statements and the Programs' individual 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 and on the Programs' individual financial statements as a whole. The information in the Revolving Fund (RF) Program financial statements in the consolidating financial statements (Schedules 1 through 4), the Salaries and Expense (S&E) Fund financial statements in the consolidating financial statements (Schedules 1 through 4), the Civil Service Retirement System (CSRS) and Federal Employees Retirement System (FERS) information in the consolidating statements of net cost (Schedule 2), the Message from the Director, Message from the CFO, Transmittal from OPM's Inspector General, Other

Information Section, and Appendix A are presented for purposes of additional analysis and are not a required part of the basic consolidated financial statements and the Programs' individual financial statements.

The information in the RF Program financial statements, the S&E Fund financial statements, and the CSRS and FERS information in the consolidating statements of net cost 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 audits 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 information in the RF Program financial statements, the S&E Fund financial statements, and the CSRS and FERS information is fairly stated in all material respects in relation to the basic consolidated financial statements and the Programs' individual financial statements as a whole.

The information in the Message from the Director, Message from the CFO, Transmittal from OPM's Inspector General, Other Information Section, and Appendix A have not been subjected to the auditing procedures applied in the audits of the basic consolidated financial statements and the Programs' individual 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 audits of the consolidated financial statements and the Programs' individual financial statements as of and for the year ended September 30, 2015, we considered OPM's internal control over financial reporting to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the consolidated financial statements and the Programs' individual financial statements, but not for the purpose of expressing an opinion on the effectiveness of OPM's internal control. Accordingly, we do not express an opinion on the effectiveness of OPM'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*.

Our consideration of internal control was for the limited purpose described in the preceding paragraph 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 have not been identified. However, as described in Exhibit I, we identified certain deficiencies in internal control that we consider to be a material weakness and the deficiencies described in Exhibit II to be a significant deficiency.

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. We consider the deficiency described in Exhibit I to be a material weakness.

A significant deficiency is a deficiency, or 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. We consider the deficiencies described in Exhibit II to be a significant deficiency.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether OPM's consolidated financial statements and the Programs' individual financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and noncompliance with which could have a direct and material effect on the determination of financial statement amounts. 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 disclosed instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards* or OMB Bulletin No. 15-02 as discussed in the following paragraph.

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 instances, as described in finding A of Exhibit I, in which OPM's financial management systems did not substantially comply with the Federal financial management systems requirements. The results of our tests of FFMIA disclosed no instances in which OPM's financial management systems did not substantially comply with applicable Federal accounting standards and the United States Government Standard General Ledger at the transaction level.

OPM's Responses to Findings

OPM's responses to the findings identified in our audits are described in Exhibits I and II. OPM's responses were not subjected to the auditing procedures applied in the audits of the consolidated financial statements and the Programs' individual financial statements and, accordingly, we express no opinion on the responses.

***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 OPM's internal control or compliance. Accordingly, this communication is not suitable for any other purpose.

KPMG LLP

Washington, DC
November 12, 2015

Exhibit I. Material Weakness

A. Information Systems Control Environment

Management is charged with the oversight and accountability for the governance of the information technology (IT) control environment, including general IT controls, and has not taken appropriate action to address ongoing pervasive deficiencies that have been identified in multiple information systems and reported to management as a significant deficiency or material weakness since fiscal year 2007.

Despite concerted efforts by OPM's Office of the Chief Information Officer (CIO) to make progress in addressing these long-standing findings, in fiscal year 2015, we continued to observe these long–standing findings in addition to other control weaknesses, as outlined below. Due to the persistence of a number of long-standing control weaknesses in OPM's information security control environment, collectively, we considered these matters to be a material weakness in internal control.

1. The current authoritative guidance regarding two-factor authentication has not been fully applied.
2. Access rights in OPM systems are not documented and mapped to personnel roles and functions to ensure that personnel access is limited only to the functions needed to perform their job responsibilities.
3. The information security control monitoring program was not fully effective in detecting information security control weaknesses. We noted access rights in OPM systems were:
    a) Granted to new users without following the OPM access approval process and inconsistently reviewed as part of the quarterly review process to confirm access approvals.
    b) Not revoked immediately upon user separation and inconsistently reviewed as part of the quarterly review process to confirm access removals.
    c) Granted to a privileged account without following the OPM access approval process.
4. A formalized system component inventory of devices to be assessed as part of vulnerability or configuration management processes was not maintained.
5. The Plan of Action & Milestones (POA&M) or similar tracking log did not track weaknesses identified from vulnerability scans.

Federal Information Process Standards 200, *Minimum Security Requirements for Federal Information and Information Systems*, and National Institute of Standards and Technology Special Publication 800-53 Revision 4, *Recommended Security Controls for Federal Information Systems*, in combination, provide a framework to help ensure that appropriate security requirements and security controls are applied by agencies to all federal information and information systems. This framework includes an organizational assessment of risk by agencies that validates the initial security control selection and determines if any additional controls are needed to protect organizational operations. The resulting set of security controls establishes a level of security due diligence for the organization. These conditions, mentioned above, reduce OPM's ability to have an effectively managed IT security program. Therefore, this may continue to increase the risk of IT systems being compromised.

Recommendations

We recommend that the OCIO, in coordination with the Office of the Chief Financial Officer (OCFO) and system owners in Program offices, develop and effectively implement the necessary corrective actions to:

1. Fully implement the current authoritative guidance regarding two-factor authentication.
2. Document and map access rights in OPM systems to personnel roles and functions, following the principle of "least privilege".

3. Enhance OPM's information security control monitoring program to detect information security control weaknesses by:
    a) Implementing and monitoring procedures to ensure system access is appropriately granted to new users, consistent with the OPM access approval process.
    b) Monitoring the process for the identification and removal of separated users to ensure that user access is removed timely upon separation; implementing procedures to ensure that user access, including user accounts and associated roles, are periodically reviewed based on the nature and risk of the system, and promptly modifying any accounts as necessary.
    c) Monitoring the process for granting privileged access to ensure that accounts with elevated privileges are approved based on business needs and enforce the concept of least privilege.
4. Continue to perform, monitor, and improve its patch and vulnerability management processes, to include maintaining an accurate inventory of devices.

Management Response

Management concurs with the finding and recommendation. OPM will develop and implement a corrective action plan to address these deficiencies in this new fiscal year.

Exhibit II. Significant Deficiency
B. Entity Level Controls Over Financial Management

Entity-level controls encompass the overall control environment throughout the entity. This includes the governance and management functions and the attitudes, awareness, and actions of those charged with governance, and management concerning the entity's internal control and its importance in the entity. Entity-level controls are often categorized as environmental controls, risk assessment, monitoring, and information and communications, as defined by the *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) (2013 version), and the Government Accountability Office (GAO) *Standard of Internal Control in the Federal Government*. These controls must be effective to create and sustain an organizational structure that is conducive to reliable financial reporting.

During fiscal year 2015, OPM reported a data breach which affected millions of Federal employees and government contractors. Based on our procedures to evaluate the potential impact of the data breach on OPM's financial statements, we noted a number of control deficiencies that are pervasive throughout the agency. Specifically, we noted:

1. OPM's risk assessment process is not designed appropriately to handle non-routine events and transactions. As a result, non-routine events and transactions that have a greater likelihood of resulting in a material misstatement in the financial statements are not always receiving an appropriate level of attention. Specifically, OPM did not fully assess and identify the risks associated with using a third party to store and maintain personally identifiable information that is a significant part of the underlying data used in calculating OPM's actuarial liabilities. The use of a service provider extends the financial reporting control environment and OPM's responsibilities for those relevant controls.
2. OPM's risk assessment processes do not have a mechanism in place to identify internal and external factors/events that would prompt OPM management to perform an evaluation of non-routine events or transactions and assess the impact on the financial statements: Specifically, we noted:
    a) The OCFO did not identify the data breach as a significant risk to the financial statements as some of the information compromised during the data breach is used in the development of the population used in the calculation of OPM's actuarial liabilities.
    b) The OCFO did not effectively communicate and coordinate with other OPM components regarding the initial evaluation of the potential impact of the data breach to the financial statements.
    c) Roles and responsibilities of OPM components that provide key financial and non-financial information for financial statement purposes were not clearly defined.
    d) The roles, responsibilities, and end-to-end processes activities between OPM components and shared-service providers are not clearly documented, communicated and monitored. In addition, there was no Authority to Operate a relevant system belonging to a shared-service provider for the period from November 29, 2014 through May 13, 2015.
    e) The OCFO did not properly apply Federal accounting standards when accounting for the liability related to identity monitoring, credit monitoring, identity restoration, and identity theft insurance.

As a result of our observations, OPM performed an analysis to determine whether the data breach compromised the integrity of the underlying data in calculating OPM's actuarial liabilities.

Weaknesses in entity-level controls may have a pervasive effect on how OPM responds to non-routine events and transactions that have a likelihood of resulting in material misstatements in the financial statements. Consequently, misstatements in the financial statements from non-routine events and transactions may not be prevented and/or detected and corrected on a timely basis.

Recommendation

We recommend that OPM perform a thorough review of their entity-level controls over financial reporting and relevant activities to identify the underlying cause of these deficiencies and take the appropriate corrective actions to strengthen controls to mitigate the risk of material misstatement when non-routine events occur.

Management Response

Management concurs with the finding and recommendation. OPM will develop and implement a corrective action plan, including skills gap analysis and a shared services governance structure, to address these deficiencies in the first quarter of this new fiscal year.