



UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Washington, DC 20415

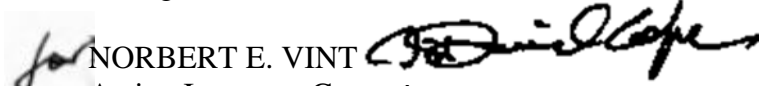
Office of the
Inspector General

November 13, 2017

Report No. 4A-CF-00-17-028

MEMORANDUM FOR KATHLEEN M. McGETTIGAN
Acting Director

FROM:


NORBERT E. VINT
Acting Inspector General

SUBJECT: Audit of the U.S. Office of Personnel Management's Fiscal Year 2017
Consolidated Financial Statements

This memorandum transmits Grant Thornton LLP's (Grant Thornton) report on its financial statement audit of the U.S. Office of Personnel Management's (OPM) Fiscal Year 2017 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 Grant Thornton to audit OPM's consolidated financial statements as of September 30, 2017, 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. 17-03, *Audit Requirements for Federal Financial Statements*.

Grant Thornton's audit report for Fiscal Year 2017 includes opinions on the consolidated financial statements and the individual statements for the three benefit programs. In addition, Grant Thornton separately reported on internal controls and on compliance with laws and regulations. In its audit of OPM, Grant Thornton found:

- The consolidated financial statements were fairly presented, in all material respects, in conformity with U.S. generally accepted accounting principles.
- Grant Thornton's internal control 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 Agency's financial statements will not be prevented, or detected and corrected, on a timely basis.

- Grant Thornton's internal control report did not identify any significant deficiencies.

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.

- Grant Thornton'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 Grant Thornton's test 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 Grant Thornton's Audit Performance

In connection with the audit contract, we reviewed Grant Thornton'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 Grant Thornton's audit of OPM's Fiscal Year 2017 Consolidated Financial Statements in accordance with GAS. Specifically, we:

- provided oversight, technical advice, and liaison to Grant Thornton 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 17-03, and other applicable professional auditing standards;
- documented oversight activities and monitored audit status;

- reviewed responses to audit reports and reported significant disagreements, if any, 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. Grant Thornton is responsible for the attached auditor's report dated November 13, 2017, and the conclusions expressed in the reports. However, our review disclosed no instances where Grant Thornton 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 Grant Thornton's audit and our oversight of the financial statement audit this year.


If you have any questions about Grant Thornton'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 [REDACTED].

cc: Dennis D. Coleman
Chief Financial Officer

Daniel K. Marella
Deputy Chief Financial Officer

David A. Garcia
Chief Information Officer

Janet L. Barnes
Director, Internal Oversight and Compliance


Chief, Policy and Internal Control



Grant Thornton LLP
1000 Wilson Boulevard., 14th Floor
Arlington, VA 22209
T 703.847.7500
F 703.848.9580
www.GrantThornton.com

REPORT OF INDEPENDENT CERTIFIED PUBLIC ACCOUNTANTS

Kathleen M. McGettigan, Acting Director
United States Office of Personnel Management

Norbert E. Vint, Acting Inspector General
United States Office of Personnel Management

Report on the financial statements

We have audited the accompanying consolidated and consolidating financial statements of the United States Office of Personnel Management (OPM) (the “Agency”), which comprise the consolidated and consolidating balance sheets as of September 30, 2017 and 2016, and the related consolidated and consolidating statements of net cost and changes in net position, and the combined and combining statements of budgetary resources for the years then ended, and the related notes to the consolidated and consolidating financial statements (collectively, the “financial statements”).

Management’s responsibility for the financial statements

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

Auditor’s responsibility

Our responsibility is to express an opinion on these 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. 17-03, *Audit Requirements for Federal Financial Statements*. Those standards and OMB Bulletin No. 17-03 require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the Agency's preparation and fair presentation of the 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 Agency'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 financial statements.

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

Opinion

In our opinion, the financial statements referred to above present fairly, in all material respects, the financial position of OPM as of September 30, 2017 and 2016, and its net cost, changes in net position, and budgetary resources for the years then ended in accordance with accounting principles generally accepted in the United States of America.

Other matters

Required supplementary information

Accounting principles generally accepted in the United States of America require that the information in Management's Discussion and Analysis (Section 1) and the combining schedule of budgetary resources by major budgetary account be presented to supplement the basic financial statements. Such information, although not a required part of the basic financial statements, is required by the Federal Accounting Standards Advisory Board and OMB Circular A-136, *Financial Reporting Requirements*, who consider it to be an essential part of financial reporting for placing the basic financial statements in an appropriate operational, economic, or historical context. This required supplementary information is the responsibility of management. We have applied certain limited procedures to the required supplementary information in accordance with auditing standards generally accepted in the United States of America. These limited procedures 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 financial statements, and other knowledge we obtained during our audit of the basic 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.

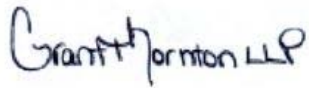
Other information

Our audit was conducted for the purpose of forming an opinion on the financial statements as a whole. The Other Information (Section 3) is presented for purposes of additional analysis and is not a required part of the basic financial statements. Such information has not been subjected to

the auditing procedures applied in the audit of the basic financial statements, and accordingly, we do not express an opinion or provide any assurance on it.

Other reporting required by *Government Auditing Standards*

In accordance with *Government Auditing Standards*, we have also issued our report, dated November 13, 2017, on our consideration of the Agency's internal control over financial reporting and on our tests of its compliance with certain provisions of laws, regulations, contracts, grant agreements and other matters. The purpose of that report is to describe the scope of our testing of internal control over financial reporting and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the Agency's internal control over financial reporting or on compliance. That report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the Agency's internal control over financial reporting and compliance.



Arlington, VA
November 13, 2017



**REPORT OF INDEPENDENT CERTIFIED PUBLIC ACCOUNTANTS
ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON
COMPLIANCE AND OTHER MATTERS REQUIRED BY *GOVERNMENT
AUDITING STANDARDS***

Grant Thornton LLP
1000 Wilson Boulevard, 14th Floor
Arlington, VA 22209
T 703.847.7500
F 703.848.9580
www.GrantThornton.com

Kathleen M. McGettigan, Acting Director
United States Office of Personnel Management

Norbert E. Vint, Acting Inspector General
United States Office of Personnel Management

We have audited, 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. 17-03, *Audit Requirements for Federal Financial Statements*, the consolidated and consolidating financial statements of the United States Office of Personnel Management (OPM) (the “Agency”), which comprise the consolidated and consolidating balance sheet as of September 30, 2017 and 2016, and the related consolidated and consolidating statements of net cost, changes in net position, and the combined and combining statement of budgetary resources for the year then ended, and the related notes to the consolidated and consolidating financial statements (collectively, the “financial statements”), and have issued our report thereon dated November 13, 2017.

Internal control over financial reporting

In planning and performing our audit of the financial statements, we considered the Agency’s internal control over financial reporting (“internal control”) to design audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of internal control. Accordingly, we do not express an opinion on the effectiveness of the Agency’s internal control.

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 Agency'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 have not been identified. We did identify certain deficiencies in internal control, described in the section titled Material Weakness – Information Systems Control Environment below that we consider to be a material weakness in the Agency's internal control.

Material Weakness – Information Systems Control Environment

In accordance with the Federal Managers' Financial Integrity Act of 1982 and the requirements of the OMB Circular A-123 *Management's Responsibility for Enterprise Risk Management and Internal Control*, Agency management is responsible for establishing and maintaining internal controls to achieve specific internal control objectives related to operations, reporting, and compliance. This includes establishing information systems controls as management relies extensively on information systems for the administration and processing of its programs, to both process and account for their expenditures, as well as for financial reporting. Lack of internal controls over these environments could compromise the reliability and integrity of the program's data and increases the risk of misstatements whether due to fraud or error.

Our internal control testing covered both general and application controls. General controls encompass the security management program, access controls (physical and logical), configuration management, segregation of duties, and service continuity or contingency planning. General controls provide the foundation for the integrity of systems including applications and the system software which make up the general support systems for an Agency's major applications. General controls, combined with application level controls, are critical to ensure accurate and complete processing of transactions and integrity of stored data. Application controls include controls over input, processing of data, and output of data as well as interface and other user controls. These controls provide assurance over the completeness, accuracy, and validity of data. Our audit included testing of OPM's mainframe, networks, databases, applications, and other supporting systems and was conducted at headquarters.

During Fiscal Year (FY) 2017, OPM made progress in strengthening controls over its information systems to address the material weakness over its information system (IS) control environment reported in FY 2016. However, our FY 2017 testing identified similar control issues in both design and operation of key controls. We believe that, in many cases, these deficiencies continue to exist because of one, or a combination, of the following:

- Risk mitigation strategies and related control enhancements require additional time to be fully implemented or to effectuate throughout the environment,
- Lack of centralized or comprehensive policies and procedures,

- The design of enhanced or newly designed controls did not completely address risks and recommendations provided over past audits, and
- Oversight and governance was insufficient to enforce policies and address deficiencies.

The information system issues identified in FY 2017 remain consistent with prior years. We also noted new deficiencies. The noted deficiencies in OPM's IS control environment in the areas of Security Management, Logical and Physical Access, and Configuration Management, in the aggregate, are considered to be a Material Weakness.

Security Management

Appropriate security management controls provide reasonable assurance that the security of an Agency's IS control environment is effective. Such controls include, amongst others, security management programs, periodic assessments and validation of risk, security control policies and procedures, and security awareness training. We noted the following deficiencies during our review of OPM's security management controls:

- System Security Plans, Risk Assessments, Security Assessment and Authorization Packages and Information System Continuous Monitoring documentation were incomplete,
- OPM did not have a centralized process in place to maintain a complete and accurate listing of systems and devices to be able to provide security oversight or risk mitigation in the protection of its resources,
- Instances of applications were not scanned during the first quarter of FY 2017 and in July 2017,
- OPM did not have a system in place to identify and generate a complete and accurate listing of OPM contractors and their employment status,
- Documentation of the periodic review of Plan of Action and Milestones (POA&Ms) did not exist,
- Several instances of known security weaknesses did not correspond to a POA&M,
- OPM did not have a system in place to identify and generate a complete and accurate listing of users with significant information systems responsibilities, and
- Entity level policies and procedures are outdated and / or incomplete.

Without a comprehensive understanding of all devices, software and systems within OPM's boundaries, OPM is unable to provide comprehensive security oversight or risk mitigation in the protection of its resources. Furthermore, without comprehensive tracking of vulnerabilities or known system weaknesses, OPM is unable to determine whether they have been remediated within a timely manner. This increases the risk of systems being compromised and may result in

the unauthorized use, modification, or disclosure of data. Further, the lack of insight into the presence of similar or aging vulnerabilities throughout all systems and devices connected to the network increases the risk of unauthorized access to sensitive information or system resources.

Logical and Physical Access

Access controls limit or detect inappropriate access to computer resources, protecting them from unauthorized modification, loss, and disclosure. Such controls include both logical and physical access controls. Logical access controls require users to authenticate themselves while limiting the files and other resources that authenticated users can access and actions they can execute. Physical access controls involve restricting physical access to computer resources and protecting them from intentional or unintentional loss or impairment. We noted the following deficiencies during our review of OPM's logical and physical access to controls:

- OPM did not comply with their policies regarding the periodic recertification of the appropriateness of user access,
- Users are not appropriately provisioned and de-provisioned access from OPM's information systems and the data center,
- Six of the six financial applications assessed were not compliant with OMB-M-11-11 *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 Policy for a Common Identification Standard for Federal Employees and Contractors* or Personal Identity Verification (PIV) and OPM policy which requires the two-factor authentication,
- Active Directory password settings were not compliant with OPM policy,
- OPM could not provide a system generated listing of all users who have access to systems,
- System roles and associated responsibilities or functions, including the identification of incompatible role assignments were not documented,
- Security events were not reviewed in a timely manner, and
- A comprehensive review of audit logs was not performed.

By not obtaining authorization for new hires and reassignments there is a risk that individuals are provided access to functions or data that is not required to perform their job responsibilities. This could allow for erroneous data entry or data changes. Further, by not removing access in a timely fashion, a terminated individual may be able to access systems or data. Finally, users who have the ability to perform functions outside of their job responsibilities or execute key processes or transactions from initiation to completion, increases the risk of inaccurate, invalid and/or unauthorized transactions being processed by the system. Therefore, there is a risk of unauthorized access to financially relevant transactions or data.

Configuration Management

Appropriate configuration management controls provide reasonable assurance that changes to information system resources are authorized, and systems are configured and operated securely and as intended. Such controls include, amongst others, effective configuration management policies, plans, and procedures; proper authorization, testing, approval, and tracking of all configuration changes; and routine monitoring of the systems configuration. We noted the following deficiencies during our review of OPM's configuration management controls:

- OPM had not developed comprehensive configuration management policies and procedures governing changes that is formally approved and disseminated to OPM personnel,
- OPM did not have the ability to generate a complete and accurate listing of modifications made to configuration items to systems,
- OPM did not maintain a security configuration checklist for platforms,
- One instance of patches were not applied in a timely manner, and
- Two instances of anti-virus were not configured or reported during the audit period.

Without formalized and comprehensive configuration management policies and procedures, the risk of having incomplete and / or inaccurate review and approval processes, audit trails of configuration changes, and configuration management documentation increases, which may in turn increase the risk that unauthorized or erroneous changes to OPM's information systems environment may be introduced without detection by system owners. Furthermore, well established configuration management controls prevent unauthorized changes to financial applications and provide reasonable assurance that systems are configured and operating securely and as intended. Included in these configuration management controls is the ability to systematically track all changes, including patches migrated or applied to the production environment. The issue noted above presents a risk that unauthorized or erroneous changes could be introduced without detection by system owners.

Recommendations

We recommend that the Office of the Chief Information Officer (OCIO), in coordination with system owners, enforce and monitor the implementation of corrective actions to:

Security Management

- Review, update and approve policies and procedures in accordance with frequencies prescribed by OPM policy,
- Implement processes to update the FISMA inventory listing to include interconnections, and review the FISMA inventory listing on a periodic basis for completeness and accuracy,
- Implement processes to associate software and hardware assets to system boundaries,

- Implement backup procedures to ensure continuous security scans over web applications,
- Implement a system or control that tracks the employment status of OPM contractors,
- Assign specific individuals with overseeing and monitoring POA&Ms to ensure security weaknesses correspond to a POA&M so that they are addressed in a timely manner,
- Establish a means of developing a complete and accurate listing of users with Significant Information System Responsibilities that are required to complete role-based training, and
- Continue to follow its project management plan to review and approve newly prepared policies so that the policies can be disseminated to stakeholders.

Logical and Physical Access

- Perform a comprehensive periodic review of the appropriateness of personnel with access to systems,
- Implement physical security access reviews to ensure access to the data center is limited to personnel that require access based on their job responsibilities,
- Implement two-factor authentication for applications,
- Document access rights to systems to include roles, role descriptions, and privileges or activities associated with each role and role or activity assignments that may cause a segregation of duties conflict,
- Ensure policies and procedures governing the provisioning and de-provisioning of access to information systems are followed in a timely manner and documentation of completion of these processes is maintained,
- Review audit logs on a pre-defined periodic basis for violations or suspicious activity and identify individuals responsible for follow up or elevation of issues to the appropriate team members for review. The review of audit logs should be documented for record retention purposes, and
- Establish a means of documenting all users who have access to systems.

Configuration Management

- Establish a comprehensive configuration management plan that includes roles and responsibilities and outlines details supporting authorization, testing and documentation requirements,
- Establish a methodology to systematically track all configuration items that are migrated to production and be able to produce a complete and accurate listing of all configuration

items for both internal and external audit purposes, which will in turn support closer monitoring and management of the configuration management process, and

- Enforce existing policy developed by OPM, vendors or federal agencies requiring mandatory security configuration settings and implement a process to periodically validate the settings are appropriate.

Views of Responsible Officials and Planned Corrective Actions

The Agency concurs with the findings and recommendations described above and will implement a corrective action plan to address these deficiencies in the new fiscal year.

Compliance and other matters

As part of obtaining reasonable assurance about whether the Agency's 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. 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.

Under the Federal Financial Management Improvement Act (FFMIA), we are required to report whether the Agency's financial management systems substantially comply with FFMIA Section 803(a) requirements. To meet this requirement, we performed tests of compliance with the federal financial management systems requirements, applicable federal accounting standards, and the *United States Government Standard General Ledger* (USSGL) at the transaction level. However, providing an opinion on compliance with FFMIA was not an objective of our audit, and accordingly we do not express such an opinion. Our work on FFMIA would not necessarily disclose all instances of lack of compliance with FFMIA requirements.

The results of our tests of FFMIA Section 803(a) requirements disclosed instances, as described above in the section titled Material Weakness – Information Systems Control Environment, 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 Section 803(a) requirements disclosed no instances of substantial noncompliance with the applicable Federal accounting standards and the USSGL at the transaction level that are required to be reported under FFMIA.

Agency's response to findings

The Agency's response to our findings, which is described in the section titled Material Weakness – Information Systems Control Environment, was not subjected to the auditing procedures applied in the audit of the financial statements, and accordingly, we express no opinion on the Agency's response.

Intended purpose

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of the Agency's internal control or on compliance. This report is an integral part of an audit

performed in accordance with *Government Auditing Standards* in considering the Agency's internal control and compliance. Accordingly, this report is not suitable for any other purpose.

Grant Thornton LLP

Arlington, VA
November 13, 2017