UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Washington, DC 20415

Office of the
Inspector General

November 15, 2018

Report No. 4A-CF-00-18-025

MEMORANDUM FOR MARGARET M. WEICHERT
Acting Director

FROM: NORBERT E. VINT
Acting Inspector General

SUBJECT: Audit of the Office of Personnel Management's Fiscal Year 2018 Closing Package Financial Statements

This memorandum transmits Grant Thornton LLP's (Grant Thornton) report on the U.S. Office of Personnel Management's (OPM) Fiscal Year 2018 Closing Package 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 Closing Package Financial Statement Reports include the Governmentwide Treasury Account Symbol Adjusted Trial Balance System (GTAS) Reconciliation Report – Reclassified Balance Sheet as of September 30, 2018; the related GTAS Reconciliation Reports – Reclassified Statement of Net Cost and Reclassified Statement of Operations and Changes in Net Position for the year then ended; and the related notes to the financial statements (hereinafter referred to as the closing package financial statements). The notes to the financial statements comprise the following:

- The GTAS Closing Package Lines Loaded Report, and
- Financial Report (FR) Notes Report (except for information in the FR Notes Report entitled "2017 – September," "Prior Year," "PY," "Previously Reported," "Line Item Changes," "Threshold," and the information as of and for the year ended September 30, 2017, in the "Text Data" of the FR Notes Reports.)

These closing package financial statements link the agency's audited consolidated financial statements to the Financial Report of the United States.

We contracted with the independent certified public accounting firm Grant Thornton to audit OPM's closing package financial statements as of September 30, 2018 and 2017. The contract requires that the audit be done in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *U.S. Government Auditing Standards*, issued by the Comptroller General of the United States; and the Office of Management and Budget (OMB) Bulletin No.19-01, *Audit Requirements for Federal Financial Statements*.

Grant Thornton reported that OPM's closing package financial statements present fairly, in all material respects, the financial position of OPM as of September 30, 2018, and its net costs and changes in net position for the year then ended in accordance with accounting principles generally accepted in the United States of America.

Grant Thornton noted no matters involving the internal control over the financial process for the closing package financial statements that are considered a material weakness or significant deficiency. Grant Thornton disclosed no instances of noncompliance or other matters that are required to be reported.

The objectives of Grant Thornton's audits of the closing package financial statements did not include expressing an opinion on internal controls or compliance with laws and regulations, and Grant Thornton, accordingly, does not express such opinions.

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 Chief Financial Officers Act for ensuring the quality of the audit work performed, we conducted a review of Grant Thornton's audit of OPM's Fiscal Year 2018 and 2017 closing package financial statements in accordance with Government Auditing Standards. 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 GAGAS, OMB Bulletin 19-01, 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 generally accepted government auditing standards, was not intended to enable us to express, and we do not express, opinions on OPM's closing package financial statements. Grant Thornton is responsible for the attached auditor's report dated November 14, 2018, and the conclusions expressed in the report. However, our review disclosed no instances where Grant Thornton did not comply, in all material respects, with auditing standards generally accepted in the United States of America.

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].

Attachment

cc: Honorable Michael J. Rigas
Deputy Director

Neal A. Patel
Acting Chief of Staff

Kathleen M. McGettigan
Chief Management Officer

Dennis D. Coleman
Chief Financial Officer

Daniel K. Marella
Deputy Chief Financial Officer

David A. Garcia
Chief Information Officer

Mark W. Lambert
Associate Director, Merit System Accountability and Compliance

Janet L. Barnes
Director, Internal Oversight and Compliance

[redacted]
Chief, Risk Management and Internal Control

Kathie Ann Whipple
Acting General Counsel

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

Margaret M. Weichert, Acting Director
United States Office of Personnel Management

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

Report on the closing package financial statements

We have audited the accompanying Closing Package Financial Statement Report of the United States Office of Personnel Management (the "Agency"), which comprises the Government-wide Treasury Account Symbol Adjusted Trial Balance System ("GTAS") Reconciliation Report – Reclassified Balance Sheet as of September 30, 2018, and the related GTAS Reconciliation Reports – Reclassified Statement of Net Cost and Reclassified Statement of Operations and Changes in Net Position for the year then ended, and the related notes to the financial statements (hereinafter referred to as the "closing package financial statements"). The notes to the financial statements comprise the following:

- the GTAS Closing Package Lines Loaded Report, and
- Financial Report ("FR") Notes Report (except for the information in the FR Notes Report entitled "2017 – September," "Prior Year," "PY," "Previously Reported," "Line Item Changes," "Threshold," and the information as of and for the year ended September 30, 2017 in the "Text Data" of the FR Notes Reports).

Management's responsibility for the closing package financial statements

Management is responsible for the preparation and fair presentation of these closing package 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 closing package 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 closing package financial statements based on our audit. We conducted our audit 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 19-01, *Audit Requirements for Federal Financial Statements*. Those standards and OMB Bulletin 19-01 require that we plan and perform the audit to obtain reasonable assurance about whether the closing package financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the closing package financial statements. The procedures selected depend on the auditor's judgment, including the assessment of the risks of material misstatement of the closing package 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 closing package 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 closing package 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 closing package financial statements referred to above present fairly, in all material respects, the financial position of the United States Office of Personnel Management as of September 30, 2018, and its net costs and changes in net position for the year then ended in accordance with accounting principles generally accepted in the United States of America.

Emphasis of matter

We draw attention to Note No. 1 to the closing package financial statements, which describes that the accompanying closing package financial statements were prepared in accordance with the requirements of the U.S. Department of the Treasury's *Treasury Financial Manual* ("TFM") Volume 1, Part 2, Chapter 4700 (*TFM 2-4700*) for the purpose of providing financial information to the U.S. Department of the Treasury and the U.S. Government Accountability Office ("GAO") to use in preparing and auditing the *Financial Report of the U.S. Government*, and are not intended to be a complete presentation of the consolidated balance sheet of the Agency as of September 30, 2018, and the related consolidated statements of net cost, changes in net position, and combined statement of budgetary resources for the year ended September 30, 2018 (hereinafter referred to as "general purpose financial statements"). The notes to the closing package financial statements are those that the U.S. Department of the Treasury deemed relevant

to the *Financial Report of the U.S. Government*. Our opinion is not modified with respect to this matter.

Other matters

Opinion on the general purpose financial statements

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 OMB Bulletin 19-01 the general purpose financial statements of the United Stated Office of Personnel Management as of and for the years ended September 30, 2018 and 2017, and our report thereon, dated November 14, 2018, expressed an unmodified opinion on those financial statements.

Required supplementary information

Accounting principles generally accepted in the United States of America require that the information, except for such information entitled "2017 – September," "Prior Year," "PY," "Previously Reported," "Line Item Changes," "Threshold," and the information as of and for the year ended September 30, 2017 included in the "Text Data" of the FR Notes Reports and "Other Text Data" of the Other Data Report, included in Other Data Report Nos. 1 (Other Data Info Section A and B only), 3 through 9, 12 (Other Data Info Section A only), 14, 17, and 18 be presented to supplement the basic closing package financial statements.

Such information, although not a required part of the basic closing package financial statements, is required by the Federal Accounting Standards Advisory Board ("FASAB"), who considers it to be an essential part of financial reporting for placing the basic closing package 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 closing package financial statements, and other knowledge we obtained during our audit of the basic closing package financial statements. Although our opinion on the basic closing package financial statements is not affected, Other Data Report Nos. 9, 17 and 18 contain material departures from the prescribed guidelines because the information included in these Other Data Reports presents the required information for the *Financial Report of the U.S. Government* and not the required information for the Agency's 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.

Management has omitted the Management's Discussion and Analysis and the combining schedule of budgetary resources by major budgetary account that accounting principles generally accepted in the United States of America require to be presented to supplement the basic closing package financial statements. Such missing information, although not a part of the basic closing package financial statements, is required by the FASAB who considers it to be an essential part of financial reporting for placing the basic closing package financial statements in an appropriate

operational, economic, or historical context. Our opinion on the basic closing package financial statements is not affected by this missing information.

Other information

Our audit was conducted for the purpose of forming an opinion on the closing package financial statements as a whole. The information other than that described in the first paragraph and the paragraph labeled *Required Supplementary Information* are presented for purposes of additional analysis in accordance with *TFM 2-4700* and are not a required part of the basic closing package financial statements. We read the other information included with the closing package financial statements in order to identify material inconsistencies, if any, with the audited closing package financial statements. Such information has not been subjected to the auditing procedures applied in the audit of the basic closing package financial statements as of and for the year ended September 30, 2018, and accordingly, we do not express an opinion or provide any assurance on it.

Restriction on use of the report on the closing package financial statements

This report is intended solely for the information and use of the management of the United States Office of Personnel Management, the U.S. Department of the Treasury, OMB, and GAO in connection with the preparation and audit of the *Financial Report of the U.S. Government* and is not intended to be and should not be used by anyone other than these specified parties.

Other reporting required by *Government Auditing Standards*

In accordance with *Government Auditing Standards* and OMB Bulletin 19-01, we have also issued our reports dated November 14, 2018, on our consideration of the Agency's internal control over financial reporting and on the results of our tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements and other matters that are required to be reported under *Government Auditing Standards*. Those reports are an integral part of an audit performed in accordance with *Government Auditing Standards* and OMB Bulletin 19-01 in considering the Agency's internal control over financial reporting and compliance, and should be read in conjunction with this report in considering the results of our audit of the closing package financial statements.

Our audit of the general purpose financial statements as of and for the year ended September 30, 2018 disclosed the following material weakness and noncompliance and other matters.

Material Weakness – Information Systems Control Environment

In accordance with the Federal Managers' Financial Integrity Act of 1982 and the requirements of the Office of Management and Budget (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 (IS) 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 FY 2018, deficiencies noted in FY 2017 continued to exist and our 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:

- 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.
- Oversight and governance was insufficient to enforce policies and address deficiencies.
- Risk mitigation strategies and related control enhancements require additional time to be fully implemented or to effectuate throughout the environment.

The information system issues identified in FY 2018 included repetitive conditions consistent with prior years as well as new deficiencies. The noted deficiencies in OPM's IS control environment in the areas of Security Management, Logical and Physical Access, Configuration Management and Interface / Data Transmission Controls, 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:

- General Support Systems (GSSs) and application System Security Plans, Risk Assessments, Authority to Operate Packages and Information System Continuous Monitoring documentation were incomplete or not reflective of current operating conditions.

- OPM did not have a centralized process in place to track 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.

- OPM did not have a system in place to identify and generate a complete and accurate listing of OPM contractors and their employment status.

- A complete and accurate listing of Plan of Action and Milestones (POA&Ms) could not be provided. Additionally, documentation of the periodic review of POA&Ms did not exist.

- OPM did not have a system in place to identify and generate a complete and accurate listing of users with significant information systems responsibility.

- Control owners were unable to articulate the IT internal control environment for one of the six in-scope applications.

Without a comprehensive understanding of all devices, software and systems and the controls that have been implemented to protect those 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 appropriate action has been taken and whether they have been remediated within a timely manner. 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. The issues presented above may increase the risk of financial systems being compromised and may result in the unauthorized use, modification, or disclosure of financially relevant transactions or data.

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, including those with privileged access, were not appropriately provisioned and de-provisioned access from OPM's information systems.

- Physical access to one of the data centers is not appropriate.

- Financial applications assessed are 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.

- Password and inactivity settings for the general support systems and one of the six in-scope applications are 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.

- A comprehensive review of audit logs was not performed for the mainframe and four of the six in-scope applications which are mainframe based, or was not performed in a timely manner for one of the six in-scope applications that resides on the network.

- Memorandums of Understandings and Interconnection Service Agreements were not reviewed on an annual basis.

- Incident handling procedures were not applied for an event identified within the agency's alert and notification tool.

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. The issues presented above may increase the risk of financial systems being compromised and may result in the unauthorized use, modification, or disclosure of 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, approved, and disseminated comprehensive configuration management policies and procedures.

- OPM did not have the ability to generate a complete and accurate listing of modifications made to configuration items to the GSS and applications.

- OPM did not maintain a security configuration checklist for platforms.

- Patches were not applied in a timely manner.

Without formalized and comprehensive configuration management policies and procedures; the inability to generate a complete and accurate listing of modifications made to production; and documentation of security configuration baselines, there is an increased risk of incomplete and / or inaccurate review and approval processes, audit trails of configuration changes, and configuration management documentation. This 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. The issue noted above presents a risk that unauthorized or erroneous changes could be introduced without detection by system owners.

Interface / Data Transmission Controls:
Interface / data transmission controls provide for the timely, accurate, and complete processing of information between applications and other feeder and receiving systems on an on-going basis. We noted the following deficiencies during our review of OPM's interface / data transmission controls:

- Controls are not in place to validate that data transmitted to applications is complete and accurate.

- Comprehensive interface / data transmission design documentation is not in place.

Without documentation specifying the data fields being transmitted from one system to another, as well as controls in place to validate that all data from the source system was transmitted to the target system in appropriate formats, incomplete or inaccurate data may transfer between systems which may impact the completeness, accuracy, and validity of data.

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 and update system documentation (System Security Plans and Authority to Operate Packages) and appropriately document results of Risk Assessments and Information System Continuous Monitoring) in accordance with agency policies and procedures.

- Enhance processes in place to track the inventory of OPM's systems and devices.

- 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, and are remediated in a timely manner.

- Establish a means of documenting a list of users with significant information system responsibilities to ensure the listing is complete and accurate and the appropriate training is completed.

- Conduct a risk assessment to identify current gaps in defining and implementing controls necessary to achieve the NIST baseline for the system. Then, develop, document, and implement controls to achieve full compliance with the baseline.

Logical and Physical Access

- 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.

- Perform a comprehensive periodic review of the appropriateness of personnel with access to systems.

- Ensure policies and procedures governing the provisioning and de-provisioning of access to the data center are followed in a timely manner and documentation of completion of these processes is maintained.

- Implement physical security access reviews to ensure access to the data center is limited to appropriate personnel.

- 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.

- 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.

- Establish a means of documenting all users who have access to systems.

- Configure password and inactivity parameters to align with agency policies.

- Review and update Interagency Service Agreements and Memorandums of Understanding in accordance with agency policies and procedures.

- Perform reconciliations to validate that all events noted within the alert and notification tool were appropriately escalated or contained a valid business justification indicating rationale for why escalation is not necessary.

Configuration Management

- Establish comprehensive configuration management policies and procedures that include roles and responsibilities and outline 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.

- 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.

- Establish a process to validate patches, updates, and fixes are applied in a timely manner.

Interface / Data Transmission Controls:

- Implement controls to validate that data transmitted to applications is complete and accurate.

- Develop interface / data transmission design documentation that specifies data fields being transmitted, controls to ensure the completeness and accuracy of data transmitted, and definition of responsibilities.

Noncompliance and Other Matters

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 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.

Internal control over financial reporting specific to the closing package financial statements

In planning and performing our audit of the closing package financial statements as of and for the year ended September 30, 2018, we also 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 an opinion on the closing package financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Agency's 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. Given these limitations, during our audit we did not identify any deficiencies in the Agency's internal control that we consider to be material weaknesses. However, material weaknesses may exist that have not been identified.

Compliance and other matters specific to the closing package financial statements

As part of obtaining reasonable assurance about whether the Agency's closing package 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 material effect on the closing package financial statements. However, providing an opinion on compliance with those provisions was not an objective of our audit of the closing package financial statements, and accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards* or OMB Bulletin 19-01.

Purpose of the other reporting required by Government Auditing Standards

The purpose of the communication provided 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 results of that testing, and not to provide an opinion on the effectiveness of the Agency's internal control or on compliance. This communication is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering internal control and compliance with provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a material effect on the closing package financial statements. Accordingly, this communication is not suitable for any other purpose.

Grant Thornton LLP

Arlington, VA
November 14, 2018