UNITED STATES OFFICE OF PERSONNEL MANAGEMENT

Washington, DC 20415

Office of the
Inspector General

November 14, 2022

Report No. 2022-IAG-003

Memorandum for The Honorable Kiran A. Ahuja, Director

From: The Honorable Krista A. Boyd
Inspector General

KRISTA BOYD Digitally signed by KRISTA BOYD
Date: 2022.11.30 14:44:48 -05'00'

Subject: Audit of the U.S. Office of Personnel Management's Fiscal Year 2022 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 2022 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 and Salaries & Expenses funds.

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, 2022 and 2021. 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. 22-01, *Audit Requirements for Federal Financial Statements*.

Grant Thornton's audit report for Fiscal Year 2022 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. The results of Grant Thornton's audit included the following:

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

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

  - Information Systems Control Environment

  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.

- Grant Thornton's 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 (FFMIA) Section 803(a), as described 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 Grant Thornton's tests of FFMIA Section 803(a) requirements disclosed no instances of substantial noncompliance with the applicable Federal accounting standards and the application of 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 2022 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 22-01, 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. Grant Thornton is responsible for the attached auditor's report dated November 14, 2022, and the conclusions expressed in the report. 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 90 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 606-2143.

Attachment

cc: Khalilah M. Harris
Chief of Staff

Dennis D. Coleman
Chief Management Officer

Benjamin C. Mizer
General Counsel

Douglas A. Glenn
Chief Financial Officer

Guy V. Cavallo
Chief Information Officer

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

Katherine M. Hax
Chief, Risk Management and Internal Control

GRANT THORNTON LLP
1000 Wilson Boulevard, 15th Floor
Arlington, VA 22209

D +1 703 847 7500
F +1 703 848 9580

REPORT OF INDEPENDENT CERTIFIED PUBLIC ACCOUNTANTS

Kiran A. Ahuja, Director
United States Office of Personnel Management

Krista A. Boyd, Inspector General
United States Office of Personnel Management

Report on the financial statements

Opinions

We have audited the consolidated financial statements of the United States Office of Personnel Management (the "Agency"), which comprise the consolidated balance sheets as of September 30, 2022 and 2021, and the related consolidated statements of net cost, changes in net position, and the combined statements of budgetary resources for the years then ended, and the related notes to the financial statements, as well as the individual balance sheets of the Retirement, Health Benefits, and Life Insurance Programs as of September 30, 2022 and 2021, and the related individual statements of net cost, changes in net position, and budgetary resources for the years then ended, and the related notes to the individual financial statements (collectively, "the individual financial statements").

In our opinion, the accompanying consolidated financial statements and individual financial statements present fairly, in all material respects, the financial position of the United States Office of Personnel Management as of September 30, 2022 and 2021, and its net cost, changes in net position, and budgetary resources for the years then ended, as well as the individual financial positions of the Retirement, Health Benefits, and Life Insurance Programs as of September 30, 2022 and 2021, and their individual net costs, 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.

Basis for opinions

We conducted our audits in accordance with auditing standards generally accepted in the United States of America (US GAAS); the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States (*Government Auditing Standards)*; and Office of Management and Budget ("OMB") Bulletin 22-01, *Audit Requirements for Federal Financial Statements*. Our responsibilities under those standards and OMB Bulletin 22-01 are further described in the Auditor's Responsibilities for the Audit of the Financial Statements section of our report. We are required to be independent of the Agency and to meet our other ethical responsibilities in accordance with the relevant ethical requirements

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

Responsibilities of management for the financial statements
Management is responsible for the preparation and fair presentation of the consolidated financial statements and individual financial statements in accordance with accounting principles generally accepted in the United States of America, and for 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 responsibilities for the audit of the financial statements
Our objectives are to obtain reasonable assurance about whether the consolidated financial statements and individual financial statements as a whole are free from material misstatement, whether due to fraud or error, and to issue an auditor's report that includes our opinions. Reasonable assurance is a high level of assurance but is not absolute assurance and therefore is not a guarantee that an audit conducted in accordance with US GAAS, *Government Auditing Standards*, and OMB 22-01 will always detect a material misstatement when it exists. The risk of not detecting a material misstatement resulting from fraud is higher than for one resulting from error, as fraud may involve collusion, forgery, intentional omissions, misrepresentations, or the override of internal control. Misstatements are considered material if there is a substantial likelihood that, individually or in the aggregate, they would influence the judgment made by a reasonable user based on the consolidated financial statements or individual financial statements.

In performing an audit in accordance with US GAAS, *Government Auditing Standards*, and OMB 22-01, we:

- Exercise professional judgment and maintain professional skepticism throughout the audit.
- Identify and assess the risks of material misstatement of the consolidated financial statements and individual financial statements, whether due to fraud or error, and design and perform audit procedures responsive to those risks. Such procedures include examining, on a test basis, evidence regarding the amounts and disclosures in the financial statements.
- Obtain an understanding of internal control relevant to the audit 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, no such opinion is expressed.
- Evaluate the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluate the overall presentation of the consolidated financial statements and individual financial statements.

We are required to communicate with those charged with governance regarding, among other matters, the planned scope and timing of the audit, significant audit findings, and certain internal control-related matters that we identified during the audit.

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 statements of budgetary resources be presented to supplement the consolidated financial statements. Such information is the responsibility of management and, although not a required part of the consolidated financial statements, is required by the Federal Accounting Standards Advisory Board and OMB Circular A-136, *Financial Reporting Requirements*, which consider it to be an essential part of financial reporting for placing the consolidated financial statements in an appropriate operational, economic, or historical context. With the exception of the Retirement, Health Benefits, and Life Insurance Programs in the combining statement of budgetary resources, on which we have expressed an opinion, we have applied certain limited procedures to the required supplementary information in accordance with US GAAS. 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 consolidated financial statements, and other knowledge we obtained during our audit of the consolidated financial statements. We do not express an opinion or provide any assurance on the information because the limited procedures do not provide us with sufficient evidence to express an opinion or provide any assurance.

Supplementary information
Our audits were conducted for the purpose of forming an opinion on the consolidated financial statements as a whole. The Revolving Fund Programs, Salaries and Expenses and Eliminations columns in the consolidating financial statements as of and for the years ended September 30, 2022 and 2021 (Schedules 1 through 3) and the Civil Service Retirement System (CSRS) and Federal Employees Retirement System (FERS) columns in the consolidating statements of net cost for the years ended September 30, 2022 and 2021 (Schedule 2) are presented for purposes of additional analysis, rather than to present the financial position and results of operations of the individual components, and are not a required part of the consolidated financial statements. Such supplementary information is the responsibility of management and was derived from and relates directly to the underlying accounting and other records used to prepare the consolidated financial statements. The information has been subjected to the auditing procedures applied in the audits of the consolidated financial statements and certain additional procedures. These additional procedures included comparing and reconciling such information directly to the underlying accounting and other records used to prepare the consolidated financial statements or to the consolidated financial statements themselves, and other additional procedures in accordance with US GAAS. In our opinion, the accompanying supplementary information is fairly stated, in all material respects, in relation to the consolidated financial statements as a whole.

Other information
Management is responsible for the other information included in the annual report. The other information comprises the Other Information presented in Section 3 but does not include the consolidated financial statements and our auditor's report thereon. Our opinion on the consolidated financial statements does not cover the other information, and we do not express an opinion or any form of assurance thereon.

In connection with our audit of the consolidated financial statements, our responsibility is to read the other information and consider whether a material inconsistency exists between the other information and the consolidated financial statements, or the other information otherwise appears to be materially misstated. If, based on the work performed, we conclude that an uncorrected material misstatement of the other information exists, we are required to describe it in our report.

Other reporting required by *Government Auditing Standards*

In accordance with *Government Auditing Standards*, we have also issued our report, dated November 14, 2022, 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.

Grant Thornton LLP

Arlington, VA

November 14, 2022

GRANT THORNTON LLP
1000 Wilson Boulevard, 15th Floor
Arlington, VA 22209

D +1 703 847 7500
F +1 703 848 9580

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

Kiran A. Ahuja, Director
United States Office of Personnel Management

Krista A. Boyd, 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 (*Government Auditing Standards*); and Office of Management and Budget ("OMB") Bulletin No. 22-01, *Audit Requirements for Federal Financial Statements*, the consolidated financial statements of the United States Office of Personnel Management (the "Agency"), which comprise the consolidated balance sheet as of September 30, 2022 and the related consolidated statements of net cost, changes in net position, and the combined statement of budgetary resources for the year then ended, and the related notes to the consolidated financial statements, as well as the individual balance sheets of the Retirement, Health Benefits, and Life Insurance Programs as of September 30 2022, and the related individual statements of net cost, changes in net position, and budgetary resources for the year then ended, and the related notes to the individual financial statements. We have issued our report, dated November 14, 2022, on these financial statements.

Report on internal control over financial reporting

Results of our consideration of internal control over financial reporting
A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the 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 were not 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 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, configuration management, segregation of duties, and backup controls. 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 organization'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 the input, processing, and output of data as well as interface 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 that reside in Macon, GA and Boyers, PA.

During FY 2022, deficiencies noted in FY 2021 continued to exist and our testing identified similar control issues in both the 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:

- Oversight and governance is 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.
- Dedicated budgetary resources are required to modernize the Agency's legacy applications.

The information system issues identified in FY 2022 included repetitive conditions consistent with prior years, as well as new deficiencies. The deficiencies in OPM's IS control environment are in the areas of Security Management, Logical Access,

Configuration Management, and Interface / Data Transmission Controls. In the aggregate, these deficiencies 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. Due to inconsistent adherence to policies and procedures related to key information system controls, we noted the following security management control weaknesses:

- General Support Systems (GSSs) and application System Security Plans, Risk Assessments, Authority to Operate Packages and Information System Continuous Monitoring documentation were incomplete, not timely, 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.
- OPM does not track vulnerabilities to remediation in accordance with policy.
- OPM did not have a system in place to identify and generate a complete and accurate listing of users with significant information systems responsibility.

Incomplete and inaccurate system documentation presents the risk that personnel do not adhere to required processes and controls, and in some cases, prohibits the auditor from testing select FISCAM domains. The lack of comprehensive and consistent continuous monitoring activities and risk assessments as well as the lack of comprehensive tracking or periodic review of vulnerabilities or known system weaknesses, present the risk that personnel do not identify and remediate weaknesses in their environment in a timely manner. Additionally, without a comprehensive understanding of all devices, software and systems and the controls, OPM is unable to provide comprehensive security oversight or risk mitigation in the protection of its resources. Furthermore, without comprehensive tracking or periodic review 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. Lastly, without comprehensive separation processes, contractors may retain lingering access to systems. 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 Access

Access controls limit or detect inappropriate access to computer resources, protecting them from unauthorized modification, loss, and disclosure. Logical access controls require users to authenticate themselves while limiting the data and other resources that authenticated users can access and actions they can execute. Due to inconsistent adherence to policies and procedures related to key information system controls, we noted the following weaknesses in logical access controls:

- Users, including those with privileged access, were not appropriately provisioned and de-provisioned access from OPM's information systems.
- OPM did not comply with their policies regarding the periodic recertification of the appropriateness of user access.
- 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 require the two-factor authentication.
- OPM could not provide a system generated listing of all users who have access to systems, as well as a listing of all users who had their access to systems revoked during the period.
- System roles and associated responsibilities or functions, including the identification of incompatible role assignments, were not documented.
- Audit logging and monitoring procedures were not developed for all tools, operating systems, and databases contained within the application boundaries. Further, a comprehensive review of audit logs was not performed, or was not performed in a timely manner.

Incomplete documentation that outlines systematic roles and responsibilities as well as segregation of duties conflicts presents the risk that individuals have access to data or the ability to perform functions outside of their job responsibilities. Additionally, the lack of proper access provisioning and termination processes as well as the lack of comprehensive recertifications of user access, may allow individuals to gain unauthorized access to systems. Lack of comprehensive audit logging and monitoring controls presents the risk that individuals perform unauthorized actions within the application without investigation and recourse. Additionally, applications not being

compliant with Personal Identity Verification (PIV) polices increases the risk of unauthorized access into systems. 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. Due to inconsistent adherence to policies and procedures related to configuration management controls, we noted the following weaknesses in configuration management controls:

- OPM did not have the ability to generate a complete and accurate listing of modifications made to configuration items to the applications.
- Users have access to both develop and migrate changes to the information systems. Additionally, there were instances in which OPM was unable to articulate users with access to develop and migrate changes to the information systems.
- OPM did not perform post-implementation reviews to validate that changes migrated to production were authorized for in scope systems.
- OPM did not maintain a security configuration checklist for platforms and did not collect baseline data to validate compliance with agency requirements Furthermore, baseline scans were not configured on all production servers within application boundaries, and misconfigurations identified through baseline scans were not remediated in a timely manner.

Well established configuration management controls prevent unauthorized changes to the application 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 that were modified and migrated to the production environment, validate that all changes migrated to production are authorized and valid, and separate development and migration duties. Additionally, without restrictive configuration settings, as well as a periodic assessment to ensure that settings are appropriate, the risk that systems are not secure increases. 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.

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. Due to inconsistent adherence to policies and procedures related to key information system controls, we noted the following control deficiency during our testing:

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

Without comprehensive documentation specifying the responsibilities of personnel involved in the interface process as well as controls in place to validate that all data from the source system was transmitted to the target system in appropriate formats, there is an increased risk that that data processing was incomplete or not restricted to appropriate personnel. Additionally, 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 (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 and validate that security software and tools are installed on all systems.
- Implement a system or control that tracks current and separated 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.

Logical 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.
- Implement two-factor authentication for applications.
- Document access rights to systems to include roles, role descriptions, privileges or activities associated with each role, and role or activity assignments that may cause a segregation of duties conflict.
- Prepare audit logging and monitoring procedures for databases within application boundaries. 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 and all users who had their systems access revoked.

Configuration Management

- Establish a mechanism to systematically track all configuration items that are migrated to production in order to produce a complete and accurate listing of all configuration items. Further, develop, document, implement, and enforce requirements and processes to periodically validate that all configuration items migrated to production are authorized and valid.
- Separate users with the ability to develop and migrate changes to production or implement controls to detect instances in which a user develops and migrates the same change.
- Enforce existing policy developed by OPM, vendors or federal agencies requiring mandatory security configuration settings, implement a process to periodically validate the settings are appropriate and ensure that proper baselines are scanned.

Interface / Data Transmission Controls:

- Develop interface / data transmission design documentation that specifies definition of responsibilities, as well as on-going system balancing requirements.

Basis for results of our consideration of internal control over financial reporting
We performed our procedures related to the Agency's internal control over financial reporting in accordance with auditing standards generally accepted in the United States of America; *Government Auditing Standards*; and OMB Bulletin No. 22-01.

Responsibilities of management for internal control over financial reporting
Management is responsible for maintaining effective internal control over financial reporting ("internal control"), including 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 responsibilities for internal control over financial reporting
In planning and performing our audit of the financial statements, we considered the Agency's internal control as a basis for designing 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. We did not consider all internal controls relevant to operating objectives, such as those controls relevant to preparing performance information and ensuring efficient operations.

Definition and inherent limitations of internal control over financial reporting
An entity's internal control over financial reporting is a process affected by those charged with governance, management, and other personnel, designed to provide reasonable assurance regarding the preparation of reliable financial statements in accordance with accounting principles generally accepted in the United States of America. An entity's internal control over financial reporting provides reasonable assurance that (1) transactions are properly recorded, processed, and summarized to permit the preparation of financial statements in accordance with accounting principles generally accepted in the United States of America, and assets are safeguarded against loss from unauthorized acquisition, use, or disposition, and (2) transactions are executed in accordance with provisions of applicable laws, including those governing the use of budget authority, regulations, contracts and grant agreements, noncompliance with which could have a material effect on the financial statements.

Because of its inherent limitations, internal control over financial reporting may not prevent, or detect and correct, misstatements due to fraud or error.

Intended purpose of report on internal control over financial reporting
The purpose of this report is solely to describe the scope of our consideration of internal control over financial reporting and the results of our procedures, and not to provide an opinion on the effectiveness of the Agency's internal control over financial reporting. This 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. Accordingly, this report on internal control over financial reporting is not suitable for any other purpose.

Report on compliance with laws, regulations, contracts, and grant agreements and other matters

As part of obtaining reasonable assurance about whether the Agency's consolidated financial statements are free from material misstatement, we performed tests of its compliance with selected provisions of applicable laws, regulations, contracts, and grant agreements consistent with the auditor's responsibility discussed below, in accordance with *Government Auditing Standards*.

Results of our tests of compliance
The objective of our tests was not to provide an opinion on compliance with laws, regulations, contracts, and grant agreements applicable to the Agency. 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 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 the Agency'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 applicable Federal accounting standards and the application of the USSGL at the transaction level.

Basis for results of our tests of compliance
We performed our tests of compliance in accordance with auditing standards generally accepted in the United States of America; *Government Auditing Standards*; and OMB Bulletin No. 22-01.

Responsibilities of management for compliance
Management is responsible for complying with laws, regulations, contracts, and grant agreements applicable to the Agency.

Auditor's responsibilities for tests of compliance
Our responsibility is to test compliance with selected provisions of applicable laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the financial statements, and to perform certain other

limited procedures. We did not test compliance with all laws, regulations, contracts, and grant agreements. Noncompliance may occur that is not detected by these tests.

Views of Responsible Officials and Planned Corrective Actions
The Agency concurs with the findings and recommendations described above and will continually implement corrective actions plans with target remediation dates in the new fiscal year. Further, the prevention and remediation of audit findings and recommendations will remain a priority for the Chief Information Officer (CIO) and Office of Chief Information Officer (OCIO). OCIO has implemented a program to continually review the status of remediation efforts.

Agency's response to findings
Government Auditing Standards requires the auditor to perform limited procedures on the Agency's response to the findings identified in our audit and described in the section titled Views of Responsible Officials and Planned Corrective Actions. The Agency's response was not subjected to the other auditing procedures applied in the audit of the consolidated financial statements, and accordingly, we express no opinion on the Agency's response.

Intended purpose of report on compliance
The purpose of this report is solely to describe the scope of our testing of compliance with selected provisions of applicable laws, regulations, contracts, and grant agreements, and the results of that testing, and not to provide an opinion on compliance. This report is an integral part of an audit performed in accordance with *Government Auditing Standards* in considering the Agency's compliance. Accordingly, this report is not suitable for any other purpose.

Grant Thornton LLP

Arlington, VA
November 14, 2022