**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. 24-01, *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, 2023 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 2023, 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 13, 2023, 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 Auditor's responsibilities for internal control over financial reporting 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 2023, deficiencies noted in FY 2022 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 are 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 2023 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 users with significant information systems responsibility.

- OPM did not perform a comprehensive and timely review of a Service Organization Controls (SOC) report.

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 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. The lack of review of the SOC report increases the risk that (a) modifications or amendments to responsibilities and controls may go undetected, and (b) required updates are not documented and implemented. This risk may impact confidentiality, integrity, or availability of financial data within the application. 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.

- OPM did not implement a required Complimentary Customer Agency Control (CCAC) regarding separated employees.

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) policies 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.

- OPM could not provide listings of users to the various environments to ensure that proper segregation of duties exist within the Configuration Management processes. (i.e. a developer cannot develop and migrate changes)

- 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.

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.

- Implement a mechanism in order to associate hardware and software assets with application boundaries.

- 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.

- Perform a review of the SOC 2 Report to ensure physical access and security controls are implemented appropriately.

**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.

- Create a process to notify the shared service provider timely of separated employees.

**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.

- Develop a process to be able to provide user listings for each environment and ensure that proper segregation of duties within these environments is enforced.

- 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. 24-01.

**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 and individual 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. 24-01.

### 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

Grant Thornton

OPM does not concur with the auditor's reported FFMIA Section 803(a) non-compliance with financial systems. OPM reported non-compliance with the FFMIA system requirements in FY 2022 due to the material weakness reported in the information system control environment. On 10/1/22, OPM migrated its mainframe-based core financial system for Trust Funds accounting, Federal Financial System (FFS), to the AIOS (ARC Integrated Oracle Solution), part of the Department of the Treasury's shared services platform. The migration of OPM's core accounting systems from legacy systems to third-party services, as well as its existing full shared services with the Department of Transportation, Federal Aviation Administration's Enterprise Service Center (ESC) transactional accounting support and Delphi platform which was migrated in 2020, allows OPM to report compliance with FFMIA and close the material weakness from the prior year.

**Grant Thornton Response**

Grant Thornton reviewed the additional context provided in management's response. Management's response does not affect the assessments of the material weakness and the substantial noncompliance with the Federal financial management systems requirements.

**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 individual 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 13, 2023