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

Independent Auditors' Report

Secretary and Inspector General
U.S. Department of Labor

Report on the Financial Statements

The accompanying financial statements of the U.S. Department of Labor (DOL) comprise the consolidated financial statements and the sustainability financial statements. We have audited the consolidated financial statements, which comprise the consolidated balance sheets as of September 30, 2018 and 2017, and the related consolidated statements of net cost, and changes in net position, and combined statements of budgetary resources for the years then ended, and the related notes to the consolidated financial statements.

We have audited the 2018 sustainability financial statements, which comprise the statements of social insurance as of September 30, 2018, 2017, 2015, and 2014; the statement of changes in social insurance amounts for the year ended September 30, 2018; and the related notes to the 2018 sustainability financial statements.

Further, we were engaged to audit the statement of social insurance as of September 30, 2016, and the related notes to this financial statement. We were also engaged to audit the statement of changes in social insurance amounts for the year ended September 30, 2017, and the related notes to this financial statement.

Management's Responsibility for the Financial Statements

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

Auditors' Responsibility

Our responsibility is to express opinions on these financial statements based on our audits. We conducted our audits of the consolidated financial statements and the 2018 sustainability financial statements in accordance with auditing standards generally accepted in the United States of America, in accordance with the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States, and in accordance with Office of Management and Budget (OMB) Bulletin No. 19-01, *Audit Requirements for Federal Financial Statements*. Those standards and OMB Bulletin No. 19-01 require that we plan and perform the audits

to obtain reasonable assurance about whether the consolidated financial statements and the 2018 sustainability financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the financial statements. The procedures selected depend on the auditors' judgment, including the assessment of the risks of material misstatement of the financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the financial statements.

We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinions on the consolidated financial statements and the 2018 sustainability financial statements.

Because of the matter described in the Basis for Disclaimer of Opinion paragraph, however, we have not been able to obtain sufficient appropriate audit evidence to provide a basis for an audit opinion on the statement of social insurance as of September 30, 2016 or the statement of changes in social insurance amounts for the year ended September 30, 2017.

Basis for Disclaimer of Opinion on the Statement of Social Insurance as of September 30, 2016 and the Statement of Changes in Social Insurance Amounts for the Year Ended September 30, 2017

As described in Note 1.W.2, DOL refined its methodology for estimating future excise tax income in fiscal year 2016. DOL was unable to provide sufficient analyses or other documentation to evidence that its methodology and certain underlying assumptions used in the determination of the present value of estimated future excise tax income for the current and new participants in the statement of social insurance as of September 30, 2016 were prepared and fairly presented in accordance with U.S. generally accepted accounting principles. Therefore, we have not been able to obtain sufficient appropriate audit evidence for the present value of estimated future excise tax income for the current and new participants.

Since the present value of estimated future excise tax income for current and new participants as of September 30, 2016 enters into the determination of the changes in social insurance amounts, we were unable to determine whether any adjustment might have been necessary in respect to the changes in assumptions about excise tax revenues and the changes in assumptions about interest rates amounts reported in the statement of changes in social insurance amounts for the year ended September 30, 2017.

Disclaimer of Opinion on the Statement of Social Insurance as of September 30, 2016 and the Statement of Changes in Social Insurance Amounts for the Year Ended September 30, 2017

Because of the significance of the matter described in the Basis for Disclaimer of Opinion paragraph, we have not been able to obtain sufficient appropriate audit evidence to provide a basis for an audit

opinion on the U.S. Department of Labor's social insurance information as of September 30, 2016, and the changes in social insurance amounts for the year ended September 30, 2017. Accordingly, we do not express an opinion on the statement of social insurance as of September 30, 2016, and the statement of changes in social insurance amounts for the year ended September 30, 2017.

Opinions on the Financial Statements

In our opinion, the consolidated financial statements referred to above present fairly, in all material respects, the financial position of the U.S. Department of Labor as of September 30, 2018 and 2017, and its net costs, changes in net position, and budgetary resources for the years then ended in accordance with U.S. generally accepted accounting principles.

Also, in our opinion, the 2018 sustainability financial statements referred to above present fairly, in all material respects, the U.S. Department of Labor's social insurance information as of September 30, 2018, 2017, 2015, and 2014; and its changes in social insurance amounts for the year ended September 30, 2018; in accordance with U.S. generally accepted accounting principles.

Emphasis of a Matter

As discussed in Notes 1-W and 1-Y to the financial statements, the sustainability financial statements are based on management's assumptions. These sustainability financial statements present the actuarial present value of DOL's future expenditures to be paid to or on behalf of participants, the present value of estimated future income to be received from excise taxes, and the present value of estimated future expenditures for administrative costs during a projection period sufficient to illustrate long-term sustainability. The sustainability financial statements are intended to aid users in assessing whether future resources will likely be sufficient to sustain public services and to meet obligations as they come due. The statements of social insurance and changes in social insurance amounts are based on income and benefit formulas in current law and assume that scheduled benefits will continue after the related trust fund is exhausted. The sustainability financial statements are not forecasts or predictions. The sustainability financial statements are not intended to imply that current policy or law is sustainable. In preparing the sustainability financial statements, management considers and selects assumptions and data that it believes provide a reasonable basis to illustrate whether current law or policy is sustainable. Assumptions underlying such sustainability information do not consider changes in policy or all potential future events that could affect future income, future expenditures, and sustainability. Because of the large number of factors that affect the sustainability financial statements and the fact that future events and circumstances cannot be estimated with certainty, even if current policy is continued, there will be differences between the estimates in the sustainability financial statements and the actual results, and those differences may be material. Our opinion on the 2018 sustainability financial statements is not modified with respect to this matter.

Other Matters

Interactive Data

Management has elected to reference to information on websites or other forms of interactive data outside the *Agency Financial Report* to provide additional information for the users of its financial statements. Such information is not a required part of the basic financial statements or supplementary information required by the Federal Accounting Standards Advisory Board. The information on these

websites or the other interactive data has not been subjected to any of our auditing procedures, and accordingly we do not express an opinion or provide any assurance on it.

Required Supplementary Information

U.S. generally accepted accounting principles require that the information in the Management's Discussion and Analysis, Required Supplementary Information, and Required Supplementary Stewardship Information sections be presented to supplement the basic financial statements. Such information, although not a part of the basic financial statements, is required by the Federal Accounting Standards Advisory Board who considers it to be an essential part of financial reporting for placing the basic financial statements in an appropriate operational, economic, or historical context. We have applied certain limited procedures to the required supplementary information in accordance with auditing standards generally accepted in the United States of America, which consisted of inquiries of management about the methods of preparing the information and comparing the information for consistency with management's responses to our inquiries, the basic financial statements, and other knowledge we obtained during our audits of the basic financial statements. We do not express an opinion or provide any assurance on the information because the limited procedures do not provide us with sufficient evidence to express an opinion or provide any assurance.

Other Information

Our audits were conducted for the purpose of forming an opinion on the basic financial statements as a whole. The information in the Message from the U.S. Secretary of Labor and Other Information sections is presented for purposes of additional analysis and is not a required part of the basic financial statements. Such information has not been subjected to the auditing procedures applied in the audits of the basic financial statements, and accordingly, we do not express an opinion or provide any assurance on it.

Other Reporting Required by *Government Auditing Standards*

Internal Control over Financial Reporting

In planning and performing our audits of the financial statements as of and for the year ended September 30, 2018, we considered DOL's internal control over financial reporting (internal control) to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of DOL's internal control. Accordingly, we do not express an opinion on the effectiveness of DOL's internal control. We did not test all internal controls relevant to operating objectives as broadly defined by the *Federal Managers' Financial Integrity Act of 1982*.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that have not been identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. We did identify certain deficiencies in internal control, described in Exhibit I, that we consider to be a significant deficiency.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether DOL's financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. 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 No. 19-01.

We also performed tests of its compliance with certain provisions referred to in Section 803(a) of the *Federal Financial Management Improvement Act of 1996* (FFMIA). Providing an opinion on compliance with FFMIA was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed no instances in which DOL's financial management systems did not substantially comply with the (1) Federal financial management systems requirements, (2) applicable Federal accounting standards, and (3) the United States Government Standard General Ledger at the transaction level.

DOL's Response to the Finding

DOL's response to the finding identified in our audit is described in Exhibit II. DOL's response was not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on the response.

Purpose of the Other Reporting Required by Government Auditing Standards

The purpose of the communication described in the Other Reporting Required by *Government Auditing Standards* section is solely to describe the scope of our testing of internal control and compliance and the results of that testing, and not to provide an opinion on the effectiveness of DOL's internal control or compliance. Accordingly, this communication is not suitable for any other purpose.

KPMG LLP

November 15, 2018

1. Lack of Sufficient Information Technology General Controls over Key Financial Feeder Systems

In fiscal year (FY) 2018, the U.S. Department of Labor (DOL) continued to make progress in developing and implementing corrective action to address certain control deficiencies that were previously identified, and continued to ensure the performance of information technology (IT) controls that functioned previously did not deteriorate. During our testing of DOL's general IT controls, we noted that DOL agencies developed and implemented appropriate corrective action that resulted in the remediation of 18 previously-reported deficiencies.

While DOL continued to make improvements, we still noted certain control deficiencies in DOL's IT control environment during our FY 2018 testing. Specifically, we identified 4 new control deficiencies and 21 previously-reported control deficiencies that were not corrected or not corrected timely across key DOL financial and support systems in four DOL agencies.

DOL's IT control environment included general and application controls and system-generated reports (information produced by the entity) that support the completeness, accuracy, and validity of financial information. We classified the control deficiencies identified into the following categories: account management, configuration management, system audit log configuration and reviews, and patch management.

Account Management

Control deficiencies related to account management and system access settings increase the risk that current employees, separated employees, and/or contractors may conduct unauthorized activities and/or obtain inappropriate disclosures of sensitive data. System access setting control deficiencies may be exploited, in either a singular fashion or in combination, by a malicious user, which may affect the confidentiality, integrity, and/or availability of DOL systems and data. The specific FY 2018 deficiencies identified in this category were as follows:

- Certain application user accounts were not timely removed for separated user;
- Certain network user accounts were not timely removed for separated users and their accounts were accessed after their separation dates;
- Contractor separation dates were not consistently maintained or monitored within department-wide Federal Human Resources listings or other consolidated listings for the timely removal of accounts of separated system users; and
- Account management controls were not consistently performed, as evidenced by roles that were improperly authorized and provisioned in conflict with separation of duties principles and insufficient access re-certifications.

Configuration Management

Controls related to configuration management are designed to provide reasonable assurance that changes to information system resources are authorized and systems are configured and operated securely and as intended. Although DOL had designed controls to establish accountability and responsibility for configuration management, including monitoring and tracking of changes, we

identified that account management controls were not consistently performed over change migrators and developers with access to perform configuration management controls, during our testing. Failure to perform access re-certifications for change migrators and developers may allow for unauthorized or inappropriate changes to be applied and remain undetected by management, resulting in lower assurance that the information system will operate as intended and that the financial data is reliable, valid, and complete.

System Audit Log Configuration and Reviews

The system audit log configuration and reviews category represents controls designed to detect unauthorized access to IT systems. Although DOL had certain detective controls in place to partially mitigate the aforementioned account management and system access settings risks, we determined through our audit procedures that certain audit logs were not monitored, reviewed timely, or independently reviewed. Additionally, evidence of audit log reviews were not consistently maintained or was insufficient. The lack of effective and timely system audit log configuration and reviews may allow for unauthorized or inappropriate activities to remain undetected by management for lengthy periods of time.

Patch Management

Controls related to patch management are designed to prevent weaknesses in IT systems from being exploited. Such controls include proactively and timely patching of related security issues, and configuring IT systems in compliance with baseline security requirements. During our FY 2018 audit procedures, we noted that certain database and operating system infrastructures were configured on unsupported or outdated versions instead of the latest supported versions from the vendors.

Not upgrading to a vendor-supported database or operating system increases susceptibility to threats and vulnerabilities developing after the databases or operating systems end of support date, which ultimately increases the risk of a compromise of the confidentiality, integrity, and availability of the data residing on the information system. Patches that are not upgraded in a timely manner or where evidence is not maintained or completed out of order may result in information leaks or system threats, which may also disrupt normal system processes, allow inappropriate access, prevent updates from being implemented, and jeopardize the integrity of financial information.

Collectively, the aforementioned IT control deficiencies pose a risk to the integrity of DOL's data, which could ultimately impact DOL's ability to accurately and timely perform its financial reporting duties. The specific nature of these deficiencies, their specific causes, and the system impacted by them, have been communicated separately to management. These deficiencies were the result of issues in the monitoring or operation of departmental procedures and controls. DOL has not yet completed all of its current corrective actions and continues to invest the necessary level of effort and resources to address issues previously reported.

The National Institute of Standards and Technology Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, the Government Accountability Office's Standards for Internal Control in the Federal Government (GAO-14-704G),

and the DOL Computer Security Handbook (CSH) define the criteria for the controls in which the deficiencies were identified.

To address the deficiencies noted above, we recommend the Chief Information Officer continue to:

a) Coordinate efforts among the DOL agencies to design and implement procedures and controls to address account management, configuration management, system audit log configuration and reviews, and patching management control deficiencies in key financial feeder systems; and
b) Monitor the agencies' progress to ensure that established procedures and controls are operating effectively and maintained.

Management's Response:

See Exhibit II for management's response

Auditors' Response:

We will conduct follow-up procedures in FY 2019 to determine whether corrective actions have been developed and implemented

U.S. Department of Labor

Office of the Chief Financial Officer
Washington, D.C. 20210

NOV 14 2018

MEMORANDUM FOR ELLIOT P. LEWIS
Assistant Inspector General for Audit

FROM: JAMES WILLIAMS
Chief Financial Officer

SUBJECT: FY 2018 Independent Auditors' Report on DOL's Financial Statements
Draft Report Number: 22-19-004-13-001

Please find the attached management's response to Draft Report No. 22-19-004-13-001, FY 2018 Independent Auditors' Report on DOL' Financial Statements.

We appreciate the opportunity to provide input and look forward to continued collaboration with the OIG audit team.

Please contact me if you have any questions.

Attachment

cc: Karen Tekleberhan, Deputy Chief Financial Officer
Bryan Slater, Assistant Secretary for Administration and Management
Gundeep Ahluwalia, Chief Information Officer

Management's Response

Fiscal Year 2018 Independent Auditors' Report

1. Lack of Sufficient Information Technology General Controls over Key Financial Feeder Systems

The Office of the Assistant Secretary for Administration and Management (OASAM) concurs in general with the aggregated findings and recommendations reported in the FY 2018 Independent Auditors' Report on DOL's Financial Statements as a *Lack of Sufficient Information Technology General Controls over Key Financial Feeder Systems.*

The Department recognizes and prioritizes the importance of implementing adequate safeguards to protect information and information systems. In the year that has passed since the completion of the FY 2017 Independent Auditor's Report on DOL's Consolidated Financial Statements, significant changes in the Office of the Chief Information Officer (OCIO)'s Information Technology (IT) environment have taken place to enhance DOL's security posture.

DOL Senior IT Leadership appreciates the independent auditor's acknowledgement of the significant steps taken by the Department to identify and mitigate or remediate the root causes of deficiencies identified. Through risk management and strategic planning, Senior IT Leadership applied risk-based decision making in the approach and implementation of corrective actions. This resulted in considerable progress by OCIO in FY 2018. DOL identified, acquired, and started implementing additional cybersecurity tools to address priority risks, with full implementation anticipated by the end of FY 2019.

OCIO has prioritized remediating the risk as a result of the identified deficiencies within its cybersecurity program relating to account management, configuration management, audit log reviews, and patch management. The Department has committed additional resources to close gaps by implementing solutions that will help further remediate the findings. Because the implementation of these solutions is still in process, however, OCIO has instituted compensating controls to reduce the risk while full implementation is being completed. OCIO is also in the process of revising its compliance and oversight process to ensure that associated DOL agencies comply with Departmental polices and procedure set forth in the Computer Security Handbook (CSH).

For FY 2019, OCIO will continue to strengthen its oversight capabilities and process of enterprise-wide remediation activities by implementing additional continuous monitoring tools and activities to identify, support, and track corrective actions to address the identified gaps.

Management responses to the specific control area deficiencies noted in the report are detailed below:

Account Management

Management concurs with the finding regarding account management.

Deficiencies in account recertification, termination, or separation of duties are a result of disparate technologies and manual processes for access management across DOL's component agencies.

In the fall of 2015, DOL implemented the Personal Identity Verification (PIV)-enforced Identification and Authentication (I&A) process. Because of the timing of the implementation, it was not assessed as part of the FY 2016 audit. However, as shown in both the FY 2017 and FY 2018 Consolidated Financial Statement Audits, there has been significant improvements resulting from the implementation of the PIV enforcement. For instance, the implementation of the PIV-enforced I&A has significantly reduced the risk associated with the untimely disablement of network accounts and unauthorized access to DOL applications.

In FY 2017, DOL acquired a leading suite of tools to give DOL the ability to implement an enterprise Identity and Access Management (IAM) solution. The solution increased security capabilities while further reducing operational risk for managing accounts. As of Q4 FY 2018, DOL has completed the implementation of the solution into the production environment. The solution will permit the centralization of access control functions such as provisioning and de-provisioning of accounts, simplified sign-on, and privileged account management. In FY 2019, DOL will continue integrating DOL applications into the solution to increase these capabilities across the DOL enterprise, thereby reducing risk, mitigating vulnerabilities, and further addressing the audit findings.

Throughout FY 2018, DOL enhanced the use of auto-generated lists of separated employees sent to Agency Information Security Officers (ISOs) for review. This process ensures accounts are disabled in a timely manner for separated users. Additionally, OCIO, HR, and the badging office revised the off-boarding and transfer process. While the process continues to be refined, it has already increased awareness and interaction with all stakeholders to ensure all personnel accounts (both federal and contractor) are managed in a timely process. Additionally, as of Q4 FY 2018, OCIO delivered the automated ability to de-provision user domain accounts. During Q1 FY 2019, OCIO expects this capability to be expanded to include all OCIO managed federal and contractor domain accounts.

System Audit Log Configuration and Reviews

Management concurs with the finding regarding system audit log configuration and reviews.

Deficiencies in system audit log configuration and reviews are a result of resource constraints needed to support a robust enterprise audit log aggregation and review process. To mitigate issues, in Q4 FY 2018, DOL completed the implementation of a Security Information and Event Management (SIEM). This facilitates log reviews by providing a central collection and

reporting point for system log data. The modernization of DOL's IT infrastructure provides increased storage and processing power needed to support the enterprise SIEM solution.

Additionally, by Q2 FY 2019, DOL plans to expand its IT workforce to include Information Systems Security Officer (ISSO) support. ISSO support staff will increase the overall IT security support for information systems by including the review of audit logs.

Patch Management and Configuration Management

Management concurs with the findings regarding configuration management and patch management.

Deficiencies in patch management and configuration management are a result of aging hardware infrastructure, application software, and personnel not adhering to standard operating procedures for patch management and configuration management.

In FY 2016, DOL revised its information security continuous monitoring (ISCM) approach with additional emphasis on patch management and configuration management within the Department's information security and risk management program documentation. Rather than applying every patch and hotfix that is released by vendors, OCIO developed a risk-based process of evaluating.

The Department's patch management processes includes risk analysis /mitigation strategies, implementation of automated tools, and a repeatable process to maintain the patch level of all enterprise computing platforms. OCIO performs weekly vulnerability scans and reports of the network. These results are analyzed in order to prioritize the patch management plan. As part of the risk mitigation strategy, OCIO reviews all risk exemption requests prior to approval by the CISO. Through the enterprise risk management process, the Department applies risk mitigating best practices consistently across all agencies to ensure all mandatory regulations and policies specific to DOL risk management are addressed. While there is still work to be done, these efforts have significantly reduced the number of vulnerabilities.

In FY 2017, OCIO started sending weekly patch and vulnerability scan reports to agencies. These results help support patch and vulnerability management and supplement the existing process. In FY 2018, DOL ensured that appropriate personnel are trained and understand the OCIO patch management process (approval, testing, implementation, and documentation).

For FY 2019, IT modernization efforts are underway to refresh outdated infrastructure. DOL has also received funding and Congressional approval to modernize an outdated legacy application. Further, OCIO is working with agencies to prioritize modernization funding opportunities of additional applications.