



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, 2017 and 2016, 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 2017 sustainability financial statements, which comprise the statements of social insurance as of September 30, 2017, 2015, 2014, and 2013; and the related notes to the 2017 sustainability financial statements.

Further, we were engaged to audit the 2016 sustainability financial statements, which comprise the statement of social insurance as of September 30, 2016, the statement of changes in social insurance amounts for the year ended 2016, and the related notes to the 2016 sustainability financial statements. 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 an opinion on these financial statements based on our audits. We conducted our audits of the consolidated financial statements and the 2017 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. 17-03, *Audit Requirements for Federal Financial Statements*. Those standards and OMB Bulletin No. 17-03 require that we plan and perform the audit to obtain reasonable assurance about whether the consolidated financial statements and the 2017 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 2017 sustainability financial statements.

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

Basis for Disclaimer of Opinion on the 2016 Sustainability Financial Statements 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 and related balances in the accompanying 2016 sustainability financial statements were prepared and fairly presented in accordance with U.S. generally accepted accounting principles. Therefore, we were unable to obtain sufficient, appropriate audit evidence for the present value of estimated future excise tax income for the current and new participants and related balances.

Because 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 2016 Sustainability Financial Statements 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 its changes in social insurance amounts for the years ended September 30, 2017 and 2016. Accordingly, we do not express an opinion on the sustainability financial statements as of and for the year ended 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, 2017 and 2016, 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 2017 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, 2017, 2015, 2014, and 2013, 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 the projection period. 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 obligation 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 2017 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 Other Information section 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 audit of the financial statements as of and for the year ended September 30, 2017, we considered the 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 opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the DOL's internal control. Accordingly, we do not express an opinion on the effectiveness of the 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*.



Our consideration of internal control was for the limited purpose described in the preceding paragraph 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. However, as described in Exhibit I and II, we identified certain deficiencies in internal control that we consider to be material weaknesses and significant deficiencies.

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. We consider the deficiencies described in Exhibit I to be material weaknesses.

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. We consider the deficiencies described in Exhibit II to be significant deficiencies.

Had we been able to perform all of the procedures necessary to express an opinion on the 2016 sustainability financial statements, the statement of changes in social insurance amounts for the year ended September 30, 2017, and the related notes to these financial statements, other matters involving internal control may have been identified and reported.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the 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. 17-03.

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 the 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.

Other Matters: On September 21, 2017, DOL's Office of Inspector General (OIG) issued report number 26-17-002-03-370, in which it concluded certain violations of the *Antideficiency Act* (ADA) had occurred related to the Job Corps' operations funds for program years 2012 and 2013. However, DOL management disagreed with the OIG's conclusion that ADA violations had occurred. The OIG and management are currently in the process of determining the actions necessary to resolve this matter. As of the date of this report, no final determination has been made.



DOL's Responses to Findings

DOL's responses to the findings identified in our audit are described in Exhibit III. DOL's responses were not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on the responses.

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 result of that testing, and not to provide an opinion on the effectiveness of the DOL's internal control or compliance. Accordingly, this communication is not suitable for any other purpose.

KPMG LLP

November 15, 2017

1. Improvement Needed in the Review of Liability Estimates

The preparation of the U.S. Department of Labor's (DOL) consolidated financial statements requires management to make certain estimates and assumptions that affect the reported amounts of liabilities and the related expenses during the reporting period. Two of these estimates are the Energy Employees Occupational Illness Compensation (EEOIC) benefits liability and the grant accrual liability. During our fiscal year (FY) 2017 audit of DOL's consolidated financial statements, we identified certain deficiencies in the management review controls over these estimates. Specifically, we noted that the management review controls were not performed at a sufficient level of detail to ensure that errors in the development of the estimates were identified and corrected. Collectively, these deficiencies increase the risk that material misstatements in DOL's consolidated financial statements will not be prevented, or detected and corrected in a timely manner. As a result of these deficiencies, we identified the following errors:

EEOIC Benefits Liability

During our testing of the EEOIC benefits liability, we identified the following errors within the actuarial model used to calculate the estimate:

- The formula that calculated the discount factor used in the discounted cash flow projection for medical payments was not updated for the current fiscal year. This resulted in an understatement of \$407 million in the calculation of the discounted liability.
- The formula used to calculate the number of individuals eligible for medical expenses in historical years contained an error that linked the "total number of individuals eligible" to the incorrect cells for FYs 2001 and 2002. This resulted in an understatement of \$267 million in the calculation of the discounted liability.

In addition to the errors above and in response to questions we raised during the audit, DOL's external actuary also determined there were errors in the formulas used to calculate the number of assumed deaths for both historical years and future years that referenced the incorrect cells in the mortality table. These errors resulted in an overstatement of \$417 million in the calculation of the discounted liability.

Grant Accrual Liability

During our testing over the grant accrual liability, we noted that the grant accrual look-back analysis improperly included 111 document IDs/footprints. The document IDs/footprints erroneously included in the look-back analysis impacted the cost ratios used to calculate the grant accrual liability as of September 30, 2017, which resulted in an understatement of \$52 million.

In addition, management's review of the grant accrual that was calculated as of September 30, 2017, did not identify that the incorrect cost ratios were used in the calculation. Management's use of the incorrect cost ratios resulted in an additional understatement of \$54 million in the grant accrual liability.

Based on our observations, we determined that the Office of Workers' Compensation Programs and the Employment Training Administration need to enhance its risk assessment process to identify and assess the accounting reporting risks for critical estimates. As a result, critical estimates did not always receive the appropriate level of attention needed to ensure errors were timely identified. Furthermore, management

Financial Section

Material Weakness Exhibit I

of these components had not implemented sufficient monitoring controls to ensure the management review controls over these estimates were operating at a level of precision to identify significant errors. Without effective controls over critical estimates, material errors may occur and go undetected by management.

The following criteria are relevant to the conditions noted above:

- The Government and Accountability Office Standards for Internal Control in the Federal Government (the Standards), Section 10.02 states:

Management designs control activities in response to the entity's objectives and risks to achieve an effective internal control system. Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives to achieve the entity's objectives and address related risks. As part of the control environment component, management defines responsibilities, assigns them to key roles, and delegates authority to achieve the entity's objectives. As part of the risk assessment component, management identifies the risks related to the entity and its objectives, including its service organizations; the entity's risk tolerance; and risk responses. Management designs control activities to fulfill defined responsibilities and address identified risk responses.

- Office of Management and Budget (OMB) Circular No. A-123, Appendix A, Section II, *Management's Responsibility for Internal Controls*, states that

Internal control over financial reporting is a process designed to provide reasonable assurance regarding the reliability of financial reporting. Reliability of financial reporting means that management can reasonably make the following assertions:

- All reported transactions actually occurred during the reporting period and all assets and liabilities exist as of the reporting date (existence and occurrence);
- All assets, liabilities, and transactions that should be reported have been included and no unauthorized transactions or balances are included (completeness); and,
- All assets and liabilities have been properly valued, and where applicable, all costs have been properly allocated (valuation).

To address the deficiencies noted above, we recommend that the Director, Office of Workers' Compensation Programs and the Acting Assistant Secretary for Employment and Training Administration:

1. Implement monitoring controls over their respective estimates to ensure management's review of the estimates are performed at a sufficient level of detail, including the underlying data, assumptions and formulas used.
2. Provide additional training as necessary to the reviewers of the estimates to ensure they fully understand the components of the estimates that should be reviewed in detail.

Management's Response: See Exhibit III for management's response.

Auditors' Response: We will conduct follow-up procedures in FY 2018 to determine whether corrective actions have been developed and implemented

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

During our FY 2017 testing of DOL's entity-level controls and general information technology controls, we identified new control deficiencies in addition to certain ones that were reported in prior years across key DOL financial and support systems. This 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. In summary, during our FY 2017 testing of significant DOL financial and support systems in the four DOL agencies responsible for them, we identified 11 new control deficiencies, and 32 previously-reported deficiencies that were not corrected or not corrected timely that remained open. However, we did note that 20 previously-reported deficiencies for which DOL agencies completed sufficient corrective action in FY 2017.

While we continued to identify deficiencies in the current year, we did note that the extent of the exceptions identified for certain controls related to user access, segregation of duties, and audit logs decreased as compared to the prior year. In addition, the DOL agencies conducted risk assessments in FY 2017 over the information technology (IT) control environment to identify the root causes of certain deficiencies that were previously identified. As a result, the agencies were able to develop and implement appropriate corrective actions to remediate them and had procedures in place to ensure the performance of key financially-relevant IT controls that functioned effectively in the past did not deteriorate.

We classified the 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 increase the risk that current employees, separated employees, and/or contractors may conduct unauthorized activities and/or obtain inappropriate disclosures of sensitive data, which may affect the confidentiality, integrity, and/or availability of DOL systems and data. The specific FY 2017 deficiencies identified in this category were as follows:

- Certain application user accounts were not timely removed for separated users;
- 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;
- Inactive accounts were not consistently disabled in a timely manner; 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 during our FY 2017 audit procedures that account management controls were not consistently performed over change migrators and developers with access to perform configuration management controls. 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 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 risks, we identified during our FY 2017 audit procedures that certain audit logs were not captured, retained, monitored, reviewed timely, or independently reviewed. Additionally, evidence of audit log reviews was 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 2017 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. We also noted that certain patches were approved and tested after the patches were implemented into the production environment. Additionally, evidence of approval, successful testing and deployment was not consistently maintained or was insufficient.

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 started to invest the necessary level of effort and resources to perform root cause analyses to address issues previously reported, and to ensure that certain IT policies and procedures are developed, implemented, and operating effectively.

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) Conduct a sufficient risk assessment to identify the root causes of identified deficiencies;
- b) Document, track, and implement milestones and corrective actions to timely remediate all identified deficiencies that have been communicated to DOL management;
- c) 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
- d) Monitor the agencies' progress to ensure that established procedures and controls are operating effectively and maintained.

Management's Response: See Exhibit III for management's response.

Auditors' Response: We will conduct follow-up procedures in FY 2018 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 15 2017

MEMORANDUM FOR: ELLIOT LEWIS
Assistant Inspector General for Audit

FROM: 
GEOFFREY KENYON
Principal Deputy Chief Financial Officer

SUBJECT FY 2017 Independent Auditors' Report on DOL's Consolidated
Financial Statements
Draft Report Number: 22-18-004-13-001

Please find attached management's response to Draft Report No.22-18-004-13-001, FY 2017 Independent Auditors' Report.

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
Edward C. Hugler, Deputy Assistant Secretary for Administration and Management
Gundeep Ahluwalia, Chief Information Officer

Management's Response
Fiscal Year 2017 Independent Auditors' Report

1. Improvement Needed in Estimate Reviews

Management recognizes its responsibility for controls over estimates related to the Energy Employees Occupational Illness Compensation Program Act (EEOICPA) benefits liability. While there are inherent uncertainties involved in the estimation of EEOIC actuarial liability, management continuously seeks to improve the estimate and takes seriously its responsibility to prevent, detect, and correct errors that could lead to material misstatements.

To this end, management has worked closely with its external actuaries to correct the errors in the EEOICPA benefits liability model noted in Exhibit I. To verify the completeness and accuracy of the corrections, the model was reviewed by multiple OWCP personnel, including economists, a statistician, and the EEOICPA program Deputy Director. In addition, a management review was conducted by the OWCP Comptroller.

Moving forward, management will review its internal controls and review procedures over the EEOICPA benefits liability estimate to ensure that errors in the model are promptly identified and corrected.

Regarding the grant accrual liability, ETA has detective controls in place that would reveal any material error in calculating the accrual ratios or the actual accrual itself, including comparison to prior quarters and review of the overall amounts and distribution of the accrual entry. ETA investigates grant accrual calculations that fall outside of management's expectation (greater than 10%). A review of the accrual data is performed to ensure that the most current data is provided and the calculation is reviewed to ensure it is accurate before posting; during this fiscal year management did not use the correct ratios for the period ending 9/30/2017.

While updates were made to the grant accrual standard operating procedures during the FY 2017 audit period, ETA agrees that further improvements can be made documenting management's assessment and review. ETA will continue to review the current standard operating procedures, identify gaps, and make any required updates. ETA will also ensure key staff are identified and properly trained to review the grant accrual calculation for accuracy. ETA agrees to have these actions completed by January 31, 2018.

Management of the Department of Labor continually seeks to improve its policies and procedures to address issues identified during the audit. During FY 2018 DOL will review and update its corrective action plan and develop remediation activities to address these needed improvements. Management appreciates the opportunity to provide input and looks forward to the continued collaboration with the OIG audit team to strengthen the Department.

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

In the year that has passed since the FY 2016 Independent Auditors' Report on DOL's Financial Statements was completed, significant changes in the OCIO's IT environment have taken place and enhanced DOL's security posture.

DOL Senior IT Leadership appreciates the independent auditors' acknowledgment of the significant steps taken by the Department to identify and mitigate or remediate the root causes of deficiencies identified since FY 2016. Through risk management and strategic planning, Senior IT Leadership applied risk based-decision making in the approach and implementation of corrective actions resulting in considerable progress in FY 2017. DOL identified, acquired, and began implementing additional cybersecurity tools to address priority risks and is on track for full implementation by the end of FY 2018.

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. 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 that will give DOL the ability to implement an enterprise Identify and Access Management (IAM) solution increasing security capabilities while further reducing operational risk for managing accounts. By Q4 FY 2018, DOL is expected to complete the implementation of these solutions, to include integrating DOL applications, leading to centralization of Access Control functions such as provisioning and de-provisioning.

Also in FY 2017, auto-generated lists of separated employees began to be sent daily to Agency ISOs for review to ensure accounts are disabled in a timely manner for separated users. Additionally OCIO began the revision of HR and badging office off boarding and transfer process. The process is expected to be completed by the end of Q2 FY 2018. In addition, DOL began the implementation of a Contractor Personnel Database (CPD) and process to monitor the onboarding and separation of all contractors supporting DOL programs. The development, documentation, and implementation of a DOL-wide process to support the CPD are planned for the end of FY 2018 Q1.

System Audit Log Configuration and Reviews

Deficiencies in system audit log configuration and reviews are a result of resource constraints and the lack of tools to support a robust enterprise audit log aggregation and review process.

In FY 2017, DOL began the implementation of a Security Information and Event Management (SIEM). The underway modernization of DOL's IT infrastructure will provide increased storage and processing power needed to support the enterprise SIEM solution. DOL plans to complete the implementation of the SIEM solution by the end of Q4 FY 2018. Additionally by Q4FY18, DOL plans to expand its IT workforce to include Information System Security Officer (ISSO) support. ISSO support staff will increase overall IT security support for information systems, to include the review of audit logs.

Patch Management and Configuration Management

Deficiencies in patch management and configuration management are a result of aging hardware infrastructure 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 much emphasis on patch management and configuration management within the Departments 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 criticality and applicability of software patches.

The Department's patch management process includes risk analysis and 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 and analyzes the results to prioritize the patch management plan. As part of a risk mitigation strategy, OCIO reviews all risk exemption requests which must be approved by the CISO. The enterprise-wide risk management process ensures that the Department applies risk mitigating best practices consistently across all agencies and that all mandatory regulations and policies specific to DOL risk management are addressed.

In FY 2017, OCIO started sending weekly patch and vulnerability scan reports to agencies to support patch and vulnerability management and supplement the existing process. In FY 2018, DOL will ensure that appropriate personnel are trained on and understand the OCIO patch management process (approval, testing, implementation, and documentation). In addition, IT modernization efforts are underway to refresh outdated infrastructure.

Overall, OCIO has taken significant steps in improving the security posture, including providing the resources and oversight to address the weaknesses outlined in the subject report while implementing processes to ensure DOL's agencies and systems adhere to its information security policies, procedures and controls. OCIO will also increase the oversight process of enterprise-wide remediation activities by implementing an enterprise cybersecurity capability portfolio and process. The enterprise cybersecurity capability portfolio will categorize capabilities under the appropriate function area and security domain, identifying supporting solutions, track capability performance measures, identify gaps in the capabilities, and track corrective actions to address the capability gaps.