U.S. Department of Labor

Office of Inspector General—Office of Audit

REPORT TO THE OFFICES OF THE CHIEF FINANCIAL OFFICER AND THE CHIEF INFORMATION OFFICER

MANAGEMENT ADVISORY COMMENTS IDENTIFIED IN AN AUDIT OF THE CONSOLIDATED FINANCIAL STATEMENTS FOR THE YEAR ENDED SEPTEMBER 30, 2021

This report was prepared by KPMG LLP, under contract to the U.S. Department of Labor, Office of Inspector General, and by acceptance, it becomes a report of the Office of Inspector General.

Carolyn R. Hantz

U.S. Department of Labor
Assistant Inspector General for Audit

Date Issued: December 20, 2021
Report Number: 22-22-004-13-001

Table of Contents

Executive Summary

KPMG LLP (KPMG), under contract to the United States Department of Labor's (DOL) Office of Inspector General (OIG), audited DOL's consolidated financial statements and its sustainability financial statements as of and for the year ended September 30, 2021, and issued its *Independent Auditors' Report* on November 19, 2021. The audit was conducted in accordance with auditing standards generally accepted in the United States of America; *Government Auditing Standards*, issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 21-04, *Audit Requirements for Federal Financial Statements*. The objective of the audit engagement was to express opinions on the fair presentation of DOL's consolidated financial statements and its sustainability financial statements.

This report presents for DOL's consideration certain matters KPMG noted, as of November 19, 2021, involving deficiencies in internal control identified during the audit. KPMG prepared this report to assist DOL in developing corrective actions for the management advisory comments identified in the Fiscal Year (FY) 2021 audit.

These management advisory comments, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies as summarized in Exhibit I. Included in this report are three comments newly identified in FY 2021 and six prior-year comments that continued to exist in FY 2021. Also included in this report are seven prior-year comments KPMG determined were corrected and closed during FY 2021. See Table 1 for a summary of comments by audit area.

Table 1: Summary of Comments by Audit Area

Audit Areas	New Comments Identified in FY 2021	Prior Year Comments Still Present in FY 2021	Prior Year Comments Closed in FY 2021
Financial Reporting	1		
Black Lung	1		
Entity Wide		1	
Human Resources			1
Unemployment Trust Fund	1		
Budget			1
Energy		1	
Grants		2	2
Information Technology		2	2
FECA			1
Totals	**3**	**6**	**7**

Source: Based on comments in Exhibit I and Exhibit II

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

November 19, 2021

Mr. Kevin Brown, Acting Chief Financial Officer
Mr. Gundeep Ahluwalia, Chief Information Officer
United States Department of Labor
Washington, DC 20210

Mr. Brown and Mr. Ahluwalia:

In planning and performing our audit of the United States Department of Labor's (DOL) consolidated financial statements and its sustainability financial statements as of and for the year ended September 30, 2021, in accordance with auditing standards generally accepted in the Unites States of America, the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States, and Office of Management and Budget (OMB) Bulletin No. 21-04, *Audit Requirements for Federal Financial Statements*, we considered DOL's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinions on these 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.

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 and/or significant deficiencies and therefore, material weaknesses and/or significant deficiencies may exist that were not identified. In accordance with *Government Auditing Standards*, we issued our report dated November 19, 2021, on our consideration of DOL's internal control over financial reporting in which we communicated certain deficiencies in internal control that we consider to be a material weakness.

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. During our audit, we identified certain deficiencies in internal control. These comments and recommendations are summarized in Exhibit I.

Prior year comments and recommendations that were closed in fiscal year 2021 are summarized in Exhibit II.

DOL's responses to the comments and recommendations identified in this letter are presented in Exhibit I. DOL's responses were not subjected to the auditing procedures applied in the audit of the consolidated financial statements and sustainability financial statements, and accordingly, we express no opinion on the responses.

The purpose of this letter is solely to describe the deficiencies in internal control identified during our audit. Accordingly, this letter is not suitable for any other purpose.

Very truly yours,

KPMG LLP

Comments and Recommendations

New Financial Comments and Recommendations Identified in Fiscal Year 2021

1. Untimely Review of Changes to Claimant Information

During fiscal year 2021, we noted the Office of Workers' Compensation Programs' (OWCP) control related to the review and approval of changes to claimant information in the Automated Support Program (ASP) system did not operate effectively to ensure the timely review of the Transaction Balancing sign-off sheet that captured a summary of changes to claimants' information that occurred during the period. Specifically, we noted four instances in which the review of the Transaction Balancing sign-off sheet did not occur within 30 days after the last day of the week covered by the Transaction Balancing sign-off sheet as required by the Division of Coal Mine Workers' Compensation (DCMW) Procedure Manual (DCMW Manual). In addition, we noted that form CM-1261, *Benefit Payment Data Entry Form*, for one of the samples was not signed by the District Director or an appropriate delegate.

OWCP's controls over the review of changes to claimant information in ASP were not sufficiently designed and implemented to ensure that the review and approval of the Transaction Balancing sign-off sheet was completed timely.

Without effective controls in place, there is an increased risk that errors in the calculation of benefit payments made to claimants will not be timely detected and corrected by management.

Section 2-1402(19)(d) of the DCMW Manual, states:

> The balancer must review the original CM-1261s and/or other data input forms and compare them to the Transaction Balance History Reports as described below so that the correction of errors can be accomplished and all transactions verified and certified as correct by close of business no later than the thirtieth day following input.

The *United States Government Accountability Office's Standards for Internal Control in the Federal Government* (GAO Standards), Principle 10, 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.

The GAO Standards, Principle 12, states:

> Management periodically reviews policies, procedures, and related control activities for continued relevance and effectiveness in achieving the entity's objectives or addressing related risks. If there is a significant change in an entity's process, management reviews this process in a timely manner after the change to determine that the control activities are designed and implemented appropriately. Changes may occur in personnel, operational processes, or information technology.

Recommendations

We recommend the Director of OWCP:

1. Reinforce existing policies and procedures requiring the completion of the review and approval of the Transaction Balancing sign-off sheet timely; and

2. Provide additional training to the reviewers regarding responsibilities and expectations when reviewing changes to claimant information to ensure reviews are completed timely and consistently.

Management's Response

OWCP Division of Coal Mine Workers' Compensation management concurs with the finding and anticipates completing the corrective action by March 31, 2022. The corrective action will entail a refresher training to walk through the CM-1261 and Transaction Balancing Reports sections of our program's Benefit Payment - Policy Manual Chapter 2-1402.

Auditors' Response

Management indicated that action will be taken to address the matters identified in this comment. Follow-up procedures will be conducted in fiscal year 2022 to determine whether corrective actions have been implemented.

2. Improvements Needed in Management's Review of Quarterly Flux Analysis

During our current year audit procedures, we noted management's review over the third quarter flux analysis of the financial statements was not operating effectively. Specifically, we noted that management's review did not ensure that explanations were documented for two items with variances that exceeded management's threshold. This occurred because adjustments were made to certain balances presented in the flux analysis and the related policies and procedures did not specify that flux analysis be reviewed again subsequent to the adjustments.

Ineffective review controls increase the risk that errors in the financial statements may not be detected and corrected in a timely manner.

The GAO Standards, Principle 3, states:

> Effective documentation assists in management's design of internal control by establishing and communicating the who, what, when, where, and why of internal control execution to personnel. Documentation also provides a means to retain organizational knowledge and mitigate the risk of having that knowledge limited to a few personnel, as well as a means to communicate that knowledge as needed to external parties, such as external auditors.

The GAO Standards, Principle 4, states:

> Management recruits, develops, and retains competent personnel to achieve the entity's objectives. Management considers the following:
>
> - Train - Enable individuals to develop competencies appropriate for key roles, reinforce standards of conduct, and tailor training based on the needs of the role.

Recommendation

We recommend that the Acting Chief Financial Officer:

3. Update the policies and procedures to ensure that when adjustments are made to the financial statements any revised variances that exceed the acceptable threshold are properly investigated and documented, and the flux analysis is reviewed again.

Management's Response

Management agrees to update the policies and procedures for financial statements to include specific wording regarding the review of flux analyses after any adjustments are made to the financial statements.

Auditors' Response

Management indicated that action will be taken to address the matters identified in this comment. Follow-up procedures will be conducted in fiscal year 2022 to determine whether corrective actions have been implemented.

3. Improvements Needed in Management's Review of Benefit Disbursement

During our current year audit procedures, we noted that the Employment and Training Administration (ETA) updated the standard operating procedures for the Unemployment Trust Fund (UTF) accounts receivable with the public estimate to specify what all should be reviewed related to the estimate and provided training to reviewers. However, management's review over the benefit disbursement estimate as of February 28, 2021, was not operating effectively. Specifically, management's review did not detect that the data used in creating the Pandemic Emergency Unemployment Compensation (PEUC) portion disbursement estimate was calculated incorrectly because of a formula error.

The exception occurred because the reviewer did not review the specific program's portion of the disbursement estimate at the appropriate level of precision due to inadequate training on how to conduct the review. Additionally, there were no monitoring controls in place to ensure that the controls operated effectively.

Ineffective review controls may result in errors in the UTF disbursement estimate going undetected, resulting in a misstatement to expenses.

The GAO Standards, Principle 4, states:

> Management recruits, develops, and retains competent personnel to achieve the entity's objectives. Management considers the following:
>
> - Train - Enable individuals to develop competencies appropriate for key roles, reinforce standards of conduct, and tailor training based on the needs of the role.

The GAO Standards, Principle 10, states:

> Management monitors the internal control system through ongoing monitoring and separate evaluations. Ongoing monitoring is built into the entity's operations, performed continually, and responsive to change.

Separate evaluations are used periodically and may provide feedback on the effectiveness of ongoing monitoring.

Recommendations

We recommend that the Principal Deputy Assistant Secretary for ETA:

4. Provide reinforcement to reviewers to ensure reviews are performed at the appropriate level of precision; and

5. Implement monitoring controls to periodically verify that management controls for estimates are operating effectively.

Management's Response

Management took immediate corrective action upon the initial discovery of the inaccurate calculation. The monitoring process has been reinforced for reviewers and preparers to ensure the proper formulas are used in both the preparation and validation of the estimates.

Auditors' Response

Management indicated that action has been taken to address the matters identified in this comment. Follow-up procedures will be conducted in fiscal year 2022 to determine whether corrective actions have been implemented.

Prior Year Financial Comments and Recommendations Still Present in Fiscal Year 2021

4. Insufficient Review of Significant Medical Bills Related to the Energy Employees Occupational Illness Compensation Program Act (EEOICPA)

During our current year audit procedures, we noted the Division of Energy Employees Occupational Illness Compensation's (DEEOIC) control to review significant medical bills (i.e., bills exceeding DEEOIC's established thresholds) was not operating effectively. Specifically, we noted that 4 of 15 significant medical bills selected for testing were not reviewed by management for accuracy and eligibility prior to payment.

The medical bill payment system was configured to automatically flag bills exceeding DEEOIC's review thresholds. The four medical bills noted above were properly flagged and placed on hold so that the service provider could obtain approval from DEEOIC to process them for payment. However, the service provider forced the bills through to payment rather than sending the bills to DEEOIC for approval. In addition, DEEOIC did

not have an effective monitoring control in place to ensure that the service organization sent all medical bills that exceeded the applicable thresholds to management for review.

Ineffective controls over the accuracy and eligibility of medical bills increases the risk of errors in benefit payments made to or on behalf of claimants.

The GAO Standards, Principle 16, states:

> Management retains responsibility for monitoring the effectiveness of internal control over the assigned processes performed by service organizations. Management uses ongoing monitoring, separate evaluations, or a combination of the two to obtain reasonable assurance of the operating effectiveness of the service organization's internal controls over the assigned process. Monitoring activities related to service organizations may include the use of work performed by external parties, such as service auditors, and reviewed by management.

Prior Year Recommendations

We recommend that the Director of OWCP:

- Continue to reinforce with the service provider the requirements to obtain DEEOIC's approval for medical bills exceeding the applicable review thresholds prior to payment; and

- Implement a monitoring control to periodically verify that the service provider has sent all medical bills over the applicable thresholds to DEEOIC management for approval prior to payment.

Management's Response

DEEOIC agrees with the Notification of Findings and Recommendations for the insufficient review of the significant medical bills. Following the findings in the FY2020 audit, DEEOIC required the Bill Pay Contractor (BPC) to suspend any bills over $30,000 and any inpatient bill over $75,000. The new directive required the BPC to suspend these bills using edit code 90391 and route them to a dedicated location in the Workers Compensation Medical Bill Portal (WCMBP) for review and approval by DEEOIC Staff.

DEEOIC put internal procedures in place for the Medical Coding Specialist (MCS) to review the bills that suspended under edit 90391 and make a recommendation to the Payment Systems Manager (PSM) as to whether the billing documents support that the treatment was for a DEEOIC accepted condition. The PSM then reviews the recommendations and if the PSM concurs with the MCS recommendations, instructs the

MCS to “force” the edit which allows the payment process to continue and the BPC to pay the bill.

By implementing this process, the DEEOIC believed that the 90391 edit process prevented the BPC from forcing the edit and paying these bills. The BPC did not advise the DEEOIC that the BPC could force this edit in their system and essentially circumvent the controls put in place to ensure only DEEOIC staff can approve these large bills. These bills did not come to DEEOIC marked as “approved” by the BPC, they entirely skipped DEEOIC review. DEEOIC did not request reports of 90391 edits or of users forcing the 90391 edit because, to our knowledge, only our MCS could force the 90391 Edit in the WCMBP and approve these payments.

Now that DEEOIC knows the BPC staff can force the edit, DEEOIC has required and is receiving a weekly report of all bills posting 90391 edits to be reconciled as part of our edit 90391 controls. Moreover, DEEOIC asked the Division of Administration and Operations (DAO) and the BPC to recommend and put in place other system controls that will ensure all bills fitting the specified criteria can only be approved for payment by DOL staff; controls DEEOIC believed had already been in place. The BPC developed such controls and implemented them as part of a 10/30/2021 system update.

Lastly, for the four Transaction Control Numbers identified as deficient, DEEOIC followed its edit 90391 process for review and approval and determined that the bills were for treatment of an accepted DEEOIC condition such that PSM would have approved payment for each of them had they been submitted to us for review prior to payment.

Auditors’ Response

Management indicated that action has been taken to address the matters identified in this comment. Follow-up procedures will be conducted in fiscal year 2022 to determine whether corrective actions have been implemented.

5. Untimely Grant Closeout

During our current year audit procedures, we noted that management’s grant closeout control did not operate effectively to ensure the timely closeout of certain expired grants and the de-obligation of remaining funds, as applicable. Specifically, we noted the Veterans’ Employment and Training Service (VETS) offices did not closeout certain grants within 365 days of their expiration. We tested a sample of 30 grants that were subject to closeout during the six-month period ended March 31, 2021, and identified four VETS grants that were still noted as open.

The closeout process for these grants was delayed because the grantees used incorrect or expired indirect cost rates on their grant closeout forms. As a result, the close-out of the grants was delayed until new cost allocation plans could be established.

Without adequate controls in place to review and close out expired grants timely, including the de-obligation of any remaining funds, undelivered orders may be overstated.

Department of Labor Manual Series (DLMS) 2 – Administration: Chapter 800 – *Grant and Procurement Management; Section 875 – Responsibilities* states:

> F. The official responsible for closeout, whether the contracting or grant officer as specified in (e) above, or the closeout unit, as specified in (d) above, is responsible for:
>
> *1.* Overseeing the timely closeout of the contract, grant, or agreement;
> *2.* Coordinating activities at closeout …;
> *3.* Scheduling and monitoring closeout activities to avoid or eliminate backlogs and to complete the closeout process within time frames established in paragraph 877, below.

DLMS 2 – Administration: Chapter 800 – *Grant and Procurement Management; Section 877 – Time Frames for Closeout*, states:

> Special circumstances may exist which delay closeout, such as a closeout following termination or a closeout where litigation or an appeal is pending. Unless such a circumstance exists, the contracting or grant officer shall close out a contract, grant, or agreement as soon as possible after completion (as defined in the DLMS 2-7, "HANDBOOK—CLOSEOUT OF CONTRACTS, GRANTS, AND AGREEMENTS"). Closeout should be accomplished within the following periods after completion:
>
> a. Firm fixed-price contracts – 6 calendar months. (Except for contracts for automatic data processing (ADP)).
> b. All other contracts – 18 calendar months.
> c. Grants and agreements – 12 calendar months.

The GAO Standards, Principle 10, states:

> Transactions are promptly recorded to maintain their relevance and value to management in controlling operations and making decisions. This applies to the entire process or life cycle of a transaction or event from its initiation and authorization through its final classification in summary

records. In addition, management designs control activities so that all transactions are completely and accurately recorded.

Prior Year Recommendations

We recommend that the Assistant Secretary for VETS:

- Enforce accountability of grant officers and closeout specialists to incentivize timely execution and process improvement;
- Continue to fully implement monitoring controls to track the status of grants during their closeout processes to ensure proper follow-up and timely execution; and
- Administer grant closeout continuous improvement trainings for all agencies to address inconsistent grant closeout implementation concerns.

Current Year Recommendation

We further recommend that the Assistant Secretary for VETS:

6. Monitor indirect cost schedule expiration dates and work with grantees to establish new cost allocation plans prior to grant closeout.

Management's Response

VETS is dependent upon every grantee to provide this information timely to their cognizant federal agency (CFA). VETS is also dependent on CFAs timely review and approval.

The Employment and Training Administration provides VETS with centralized grants administration services, as outlined in an existing Memorandum of Understanding. ETA's services include management of the grant closeout process following applicable regulations. ETA and VETS remain committed to their routine communication on the closeout status of all VETS grants and will continue their close collaboration on those grants exhibiting issues that may lead to significant delays in closeout. As ETA reported previously, three grants identified in this report have all experienced closeout delays due to indirect cost rate documentation. Like VETS, ETA is dependent upon every grantee to provide to their cognizant agency timely information regarding approved indirect cost rates. Additionally, the fourth grant cited in this report continues to be impacted by unique delays resultant from technical issues regarding repayment of

disallowed costs. ETA is working with partners at the Department of Health and Human Services to track down this refund in the Payment Management System.

The Department of Labor is transitioning to a new grants management system, GrantSolutions (GS). GS does not have email notifications for closeout processes. VETS has agreed to the additional cost to have this enhancement designed for VETS. VETS will go live in the grants management module in GS in the summer of 2022, this enhancement will be designed and implemented in 2023. Until then, VETS will continue with the manual process of the entire closeout process.

VETS will continue to administer grant closeout training for its staff and grantees.

VETS does and will continue to monitor indirect cost expiration dates, provide training, and administer technical assistance. However, VETS does not establish Negotiated Indirect Cost Rate Agreements (NICRAs) and/or cost allocation plans (CAPs). When DOL is the CFA, the Cost & Price Determination Division sets the NICRA or CAP for grantees. The process typically includes a back and forth process between the grantee and the CFA. This annual process applies for the life of the Federal award. Considering the timeframes involved, final rates for all grant award applicable periods may not be available during the closeout process.

Auditors' Response

Management indicated that action will be taken to address the matters identified in this comment. Follow-up procedures will be conducted in fiscal year 2022 to determine whether corrective actions have been implemented.

6. Improper Controls over Delinquent Grant Cost Reports

During our current year audit procedures, we noted that management's controls over ETA-9130 cost reports did not operate effectively to ensure the timely posting of grants expenses based on our current year audit procedures. Specifically, we noted that Federal Project Officers (FPO) were not accepting ETA-9130s (i.e., cost reports) within 10 days after they were received from the grantees. We noted for 1 of the 15 sample items selected for testing as of March 31, 2021, the FPO was delinquent in accepting the cost report once it was submitted by the grantees. The cost report was accepted 18 days late.

In addition, we determined that the FPOs did not effectively follow-up with certain grantees to ensure submission of their delinquent cost reports for 2 of the 15 sample items.

ETA developed a formal corrective action plan (CAP) to resolve or mitigate the issues, but the CAP was not consistently implemented to prevent continued control deviations.

Failure to properly remediate grantee related financial matters or to timely review and accept submitted grant expenditure details may lead to the misstatement of grant-related expenses, advances, payables, and undelivered orders.

DOL's *Grants Management Policies and Responsibilities within the Employment and Training Administration Attachment B* dated September 19, 2017 states:

> After a grantee submits a certified 9130, ETA assigned staff has 10 business days to review and accept or reject the 9130.

The GAO Standards, Principle 5, states:

> Management, with oversight body, takes corrective action as necessary to enforce accountability for internal control in the entity. These actions can range from informal feedback provided by the direct supervisor to disciplinary action taken by the oversight body, depending on the significance of the deficiency to the internal control system.

The GAO Standards, Principle 10, states:

> Transactions are promptly recorded to maintain their relevance and value to management in controlling operations and making decisions. This applies to the entire process or life cycle of a transaction or event from its initiation and authorization through its final classification in summary records. In addition, management designs control activities so that all transactions are completely and accurately recorded.

Prior Year Recommendations

We recommend that the Assistant Secretary for ETA:

- Provide continued training to FPOs, emphasizing the revised expectations of the corrective action plan;
- Enforce accountability of the FPOs to facilitate timely and successful remediation of delinquent grant cost reports; and
- Enhance monitoring controls to track the status of delinquent cost reports to ensure timely acceptance by the FPOs.

Management's Response

ETA will continue with the corrective action as outlined in the response to last year's audit and in line with the review of this year's audit findings. ETA believes that the corrective action it implemented has reduced the number of reports dramatically, and as explained to both sets of auditors, required time to implement. ETA's acceptance rate is in the very high 90's. ETA will continue using a centralized point of contact to review 9130 reports weekly and submit to Regional Offices for action. ETA will supplement this corrective action by tracking each week staff that have had late reports for elevation and corrective action in the appropriate office.

Auditors' Response

Management indicated that action will be taken to address the matters identified in this comment. Follow-up procedures will be conducted in fiscal year 2022 to determine whether corrective actions have been implemented.

7. Improvements Needed in Management's Process for Identifying, Assessing, and Responding Entity-Wide Risks

During our testing of entity-level controls, we noted that management did not conduct a department-wide risk assessment during fiscal year 2021. This occurred because management was in the process of implementing a revised Enterprise Risk Management (ERM) process that would require individual agencies to uniformly and consistently document how they identify, assess, and respond to risks. The revised ERM process was not finalized until October 2021. As a result, the individual agency's risk assessments, which were needed to complete the agency-wide risk assessment, were not completed until the first quarter of fiscal year 2022.

Without appropriately designed and implemented controls to identify, analyze, and respond to risks across DOL as a whole, management may not be able to sufficiently mitigate risks that may impact the financial statements.

The GAO Standards, Principle 7, states:

> Management identifies risks throughout the entity to provide a basis for analyzing risks. Risk assessment is the identification and analysis of risks related to achieving the defined objectives to form a basis for designing risk responses.
>
> Risks may be analyzed on an individual basis or grouped into categories with related risks and analyzed collectively. Regardless of whether risks are analyzed individually or collectively, management considers the correlation among different risks or groups of risks when estimating their

> significance. The specific risk analysis methodology used can vary by entity because of differences in entities' missions and the difficulty in qualitatively and quantitatively defining risk tolerances.

The GAO Standards, Principle 9, states:

> As part of risk assessment or a similar process, management identifies changes that could significantly impact the entity's internal control system. Identifying, analyzing, and responding to change is similar to, if not part of, the entity's regular risk assessment process. However, change is discussed separately because it is critical to an effective internal control system and can often be overlooked or inadequately addressed in the normal course of operations.

Prior Year Recommendation

The open prior year recommendation was modified. See Recommendation 7 below.

Recommendation

We recommend that the Acting Chief Financial Officer:

7. Continue their efforts to fully implement the revised ERM process and ensure that all necessary risk assessments are completed at both the individual agency level and at the agency-wide level.

Management's Response

OCFO management, in conjunction with DOL agencies, will continue our efforts to fully implement the revised ERM process and ensure that all necessary risk assessments are completed at both the individual agency level and at the agency-wide level.

Auditors' Response

Management indicated that action will be taken to address the matters identified in this comment. Follow-up procedures will be conducted in fiscal year 2022 to determine whether corrective actions have been implemented.

Prior Year Information Technology Comments and Recommendations Still Present in Fiscal Year 2021

8. Improvements Needed in Account and Configuration Management

During our current year audit procedures, we identified deficiencies associated with account and configuration management with certain DOL systems as follows:

- Certain new users were improperly authorized and provisioned before approval had been granted or without appropriate documentation;
- Certain reports used for re-certifications were not designed to capture all required users;
- Certain application and network user accounts were not timely removed for separated users or modified for existing user accounts; and
- Certain password configuration controls were not in compliance with DOL requirements.

These deficiencies were the result of issues in the monitoring, design, or operation of departmental procedures and controls. Control deficiencies related to account and configuration 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 nature of these deficiencies, their specific causes, and the system impacted by them, have been communicated separately to management.

The GAO Standards, Principle 11, states:

> Security management includes the information processes and control activities related to access rights in an entity's information technology, including who has the ability to execute transactions. Security management includes access rights across various levels of data, operating system (system software), network, application, and physical layers. Management designs control activities over access to protect an entity from inappropriate access and unauthorized use of the system. These control activities support appropriate segregation of duties. By preventing unauthorized use of and changes to the system, data and program integrity are protected from

malicious intent (e.g., someone breaking into the technology to commit fraud, vandalism, or terrorism) or error.

…

Management designs control activities for security management of the entity's information system for appropriate access by internal and external sources to protect the entity's information system. Objectives for security management include confidentiality, integrity, and availability. Confidentiality means that data, reports, and other outputs are safeguarded against unauthorized access. Integrity means that information is safeguarded against improper modification or destruction, which includes ensuring information's nonrepudiation and authenticity. Availability means that data, reports, and other relevant information are readily available to users when needed.

Prior Year Recommendations

We recommend that the Chief Information Officer:

- Coordinate efforts among the DOL agencies to design and implement procedures and controls to address account and configuration management, in key financial feeder systems; and

- Monitor the agencies' progress to ensure that established procedures and controls are operating effectively and maintained.

Management's Response

Management concurs with the recommendations. OCIO has updated its procedures surrounding account management and configuration settings for DOL systems. In addition, access controls are monitored and reviewed via the account recertification process to ensure adherence with the policy defined in DOL CSH. OCIO will continue to work with agencies to ensure that remaining corrective actions are implemented and maintained in accordance with the Department's policy.

Auditors' Response

Management indicated that action has been taken to address the matters identified in this comment. Follow-up procedures will be conducted in fiscal year 2022 to determine whether corrective actions have been implemented.

9. Improvements Needed in Patch Management

During our current year audit procedures, we identified instances in which certain controls related to patch management requirements were not operating effectively. As a result, we noted certain database and operating system infrastructures were configured on unsupported or outdated versions instead of the vendors' latest supported versions.

Office of the Chief Information Officer (OCIO) management informed us that this occurred because they accepted the risk of not remediating outstanding vulnerabilities, however, they did not formally document that decision because of competing priorities.

Controls related to patch management are designed to prevent weaknesses in information technology (IT) systems from being exploited. IT control deficiencies pose a risk to the integrity, availability, or confidentiality 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(s) impacted by them, have been communicated separately to management.

The GAO Standards, Principle 11, states:

> Management evaluates security threats to information technology, which can be from both internal and external sources. External threats are particularly important for entities that depend on telecommunications networks and the Internet. External threats have become prevalent in today's highly interconnected business environments, and continual effort is required to address these risks. Internal threats may come from former or disgruntled employees. They pose unique risks because they may be both motivated to work against the entity and better equipped to succeed in carrying out a malicious act as they have greater access to and knowledge of the entity's security management systems and processes.
>
> …
>
> Management designs control activities for security management of the entity's information system for appropriate access by internal and external sources to protect the entity's information system. Objectives for security management include confidentiality, integrity, and availability. Confidentiality means that data, reports, and other outputs are safeguarded against unauthorized access. Integrity means that information is safeguarded against improper modification or destruction, which includes ensuring information's nonrepudiation and authenticity. Availability means that data, reports, and other relevant information are readily available to users when needed.

Prior Year Recommendation

The open prior year recommendation was modified. See Recommendation 8 below.

Current Year Recommendations

We further recommend the Chief Information Officer

8. Enhance vulnerability scanning monitoring controls and procedures to track and remediate outstanding vulnerabilities in a timely manner; and

9. Formally document decisions in a memorandum when accepting the risks of not remediating findings and obtain the necessary approvals from management.

Management's Response

Management concurs with the recommendations and continues to streamline its efforts to address the recommendations. During FY 2021, outstanding vulnerabilities were remediated and updates were made to the management procedures. In addition, OCIO continues to monitor for systems with outdated patches and are taking steps to refine our vulnerability remediation strategy. For vulnerabilities that cannot be remediated within the defined timeframe, a Plan of Action and Milestones and/or a risk waiver will be created to address the vulnerability.

Auditors' Response

Management indicated that action has been taken to address the matters identified in this comment. Follow-up procedures will be conducted in fiscal year 2022 to determine whether corrective actions have been implemented.

Prior Year Comments and Related Recommendations Closed in Fiscal Year 2021

The following comments reported in the *Management Advisory Comments Identified in an Audit of the Consolidated Financial Statements for the Year Ended September 30, 2020*, dated November 16, 2020, were closed in fiscal year (FY) 2021.

Prior Year Comment Number	Fiscal Year Comment Originated	Title of Comment Reported in FY 2020 MAC	Recommendation(s) Reported in the FY 2020 MAC
2020-03	2020	Insufficient Quality Control Review of Medical Payments	We recommend that the Director of OWCP: 4. Complete follow-up actions to determine the correct amount of the medical payments and the appropriate resolution of any differences; and 5. Provide additional training to the MCS to address the deficiency identified.
2020-04	2020	Ineffective Controls over Management's Preparation and Review of Budget Compliance Analysis and Reconciliation	6. We recommend that the Chief Financial Officer update its policies and procedures to require a review over the completeness and accuracy of continuing resolution amounts used in the SF-132 compliance analysis and the SF-132 to SF-133 reconciliation.

Prior Year Comment Number	Fiscal Year Comment Originated	Title of Comment Reported in FY 2020 MAC	Recommendation(s) Reported in the FY 2020 MAC
2020-05	2020	Improvements Needed in the Review of Separated Employees	We recommend that the Assistant Secretary for Administration and Management: 7. Develop and implement policies and procedures to address the enforcement and monitoring of the control requirement for the employee separation process; and 8. Provide trainings to the applicable personnel that reinforce the separated employee process and emphasize established timeframes on the separation clearance form.
2020-08	2015	Ineffective Controls over Onsite Monitoring Reports	We recommend that the Assistant Secretary for ETA: 15. Provide continued training to FPOs, emphasizing the revised expectations of the corrective action plan; 16. Enforce accountability of the FPOs to facilitate timely issuance of final site monitoring reports and completion of required GEMS documentation; and 17. Continue to fully implement monitoring controls to ensure timely issuance of final site monitoring reports and completion of required GEMS documentation.

Prior Year Comment Number	Fiscal Year Comment Originated	Title of Comment Reported in FY 2020 MAC	Recommendation(s) Reported in the FY 2020 MAC
2020-09	2017	Untimely Issuance of Single Audit Determination Letters	We recommend the Assistant Secretary for VETS: 18. Formalize the VETS SOP for the single audit process, and include a timeline to ensure that responses are provided within the 180-day timeframe; 19. Provide continued training to staff, emphasizing the revised expectations of the corrective action plan; and 20. Enforce accountability of staff to facilitate timely issuance of Single Audit Final Determination Letters and completion of required documentation.
2020-11	2019	Improvements Needed in IT Segregation of Duties	• We recommend that the Chief Information Officer design and implement procedures to enforce separation of duties among users assigned access to the infrastructure layers to the extent possible. When not possible, an approved risk exemption waiver should be obtained, and effective monitoring controls should be developed and implemented.
2020-12	2019	Improvements Needed in Audit Log Configurations and Reviews	We recommend that the Chief Information Officer: • Segregate permissions such that production system administrators who have their privileged activities logged are not able to modify, update, or delete source log data to the extent possible and if not possible, include this risk consideration in a formal, signed risk exemption waiver.

The following comment reported in the *Management Advisory Comments Identified in an Audit of the Consolidated Financial Statements for the Year Ended September 30, 2020*, dated November 16, 2020, was partially re-issued during FY 2021 but included recommendations that were closed during the year.

Prior Year Comment Number	Fiscal Year Comment Originated	Title of Comment Reported in FY 2020 MAC	Recommendation(s) Reported in the FY 2020 MAC
2020-01	2020	Improvements Needed in Management's Entity-Wide Risk Assessment Process	1. We recommend that the Chief Financial Officer, in conjunction with management of other key agencies within DOL, enhance the related policies and procedures to clarify how agencies should perform and document their identification, assessment, and response to risks, and how DOL should aggregate and assess those risks for the entity as a whole.
2020-13	2019	Improvements Needed in Patch Management	We recommended that the Chief Information Officer: • Maintain a current and accurate population of production servers and work with system owners to update that population when server transitions or changes occur outside of any regularly scheduled maintenance updates and • Enhance vulnerability scanning monitoring controls and procedures for vulnerability scanning and patches to track and remediate outstanding vulnerabilities and patches in a timely manner and maintain supporting documentation.

Appendix A

Acronyms and Abbreviations

ADP	Automatic Data Processing
ASP	Automated Support Program
CAP	Corrective Action Plan
CFO	Chief Financial Officer
DCMW Manual	Division of Coal Mine Worker's Compensation Procedure Manual
DEEOIC	Division of Energy Employees Occupational Illness Compensation
DLMS	Department of Labor Manual Series
DOL	U.S. Department of Labor
EEOIC	Energy Employees Occupational Illness Compensation
ERM	Enterprise Risk Management
ETA	Employment and Training Administration
FAR	Federal Acquisition Regulation
FPO	Federal Project Officer
FY	Fiscal Year
GAO	Government Accountability Office
GAO Standards	Government Accountability Office's *Standards for Internal Control in the Federal Government*
IT	Information Technology
KPMG	KPMG LLP
No.	Number
OCFO	Office of the Chief Financial Officer
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OWCP	Office of Workers' Compensation Program
PEUC	Pandemic Emergency Unemployment Compensation
SOP	Standard Operating Procedures
Treasury	U.S. Department of the Treasury
UDO	Undelivered Orders
U.S.	United States
VETS	Veterans' Employment and Training Service

REPORT FRAUD, WASTE, OR ABUSE
TO THE DEPARTMENT OF LABOR

Online
http://www.oig.dol.gov/hotline.htm

Telephone
(800) 347-3756 or (202) 693-6999

Fax
(202) 693-7020

Address
Office of Inspector General
U.S. Department of Labor
200 Constitution Avenue, NW
Washington, DC 20210