Office of Inspector General

U.S. Department of Labor
Office of Information Technology Audits

DOLAR$ APPLICATION CONTROL REVIEW

Department of Labor
Office of Chief Financial Officer

Report Number: 23-02-003-13-001
Date Issued: March 29, 2002

U.S Department of Labor—Office of Chief Financial Officer
DOLAR$ Application Review

Table of Contents

Executive Summary

The Office of Inspector General (OIG) conducted a review of the automated controls over the Department of Labor Accounting and Related Systems (DOLAR$) application. The information contained in the report can be used as input by Department of Labor's (DOL) application accrediting authority for the certifying and accrediting of the DOLAR$ application.

At the beginning of the review, data flow diagrams (DFDs) for the Core, Accounts Payable and Accounts Receivable subsystems of DOLAR$ were created. These DFDs documented the critical processes and location of key computer-related controls. Using information from the DFDs, a matrix for testing and evaluating specific controls was created and approved. These critical processes and controls were tested in the areas of (1) Access, (2) Input, (3) Processing, (4) Rejection, and (5) Output.

In summary, we found two main areas for concern:

1. Security management of DOLAR$ is weakened by a lack of policies and procedures and effective monitoring and maintenance of user accounts (Access Controls). More specifically, we identified the following:
    - user account management weaknesses (i.e., security policies and procedures have not been implemented, users' access levels not commensurate with their assigned job responsibilities and user IDs for security users have not been adequately established to provide accountability and to prevent incompatibility in duties); and
    - technical control weaknesses over user access and password management.

2. The accuracy, completeness and integrity of the information processed and stored by the DOLAR$ application is weakened by inadequate application functionality (Input, Processing and Rejection Controls). More specifically, we identified the following:
    - DOLAR$ audit trail only retains the last change in the record edit history;
    - Vendor Maintenance Table is not being adequately controlled;
    - prior month posting capabilities do not provide adequate controls to prevent transactions from posting to the incorrect period; and
    - controls over the upper limit of a dollar amount that can be entered for each transaction are inadequate.

To improve controls over the DOLAR$ application, we recommend the CFO:

- develop or modify policies and procedures in the areas of access controls and the recertification process;
- utilize the DOLAR$ User Class / profile to administer access controls;
- implement an automated password management;
- increase the controls of the current manual monitoring effort;
- review and disable transaction codes to limit potential security vulnerabilities;
- add additional audit trail information;
- review Vendor Maintenance Table access for business need;
- implement periodic reviews to identify and remove duplicative, inactive and unauthorized vendors; and
- implement controls over the upper limit of a dollar amount that can be entered for each transaction.

In response to the draft report, the Acting CFO agreed to develop or modify policies and procedures in the areas of access controls and the recertification process and to implement an automated password management. However, the Acting CFO stated that the current system of assigning and controlling access provided the "granularity" needed to meet the Department's business need.

The Acting CFO generally disagreed with the conditions and / or the recommendations dealing with the application functionality. In regards to the audit trails, the Acting CFO states that some of DOLAR$ processes now have sufficient audit trails, since they have implemented the recommendation to disable the "TLCC" transaction code. The Acting CFO disagreed with the finding that a weakness exists in the current access levels to Vendor Maintenance Table. The Acting CFO also disagreed with the recommendation to review and place reasonable limits on the amount field as it would hinder DOL's ability to process timely and efficient payments and transactions.

The OIG was not provided any additional information to change or modify its position on the finding and recommendations presented in this report. We commend the Office of the Chief Financial Officer (OCFO) for the actions that have been taken to resolve some of these issues. We will continue to work with the OCFO to resolve those issues on which we currently disagree.

Background

This audit was conducted in support of the mandatory audit of DOL's Consolidated Financial Statements, as required by the Chief Financial Officers Act of 1990 (CFO Act) (P.L. 101-576). Office of Management and Budget Bulletin No. 98-08, establishes that when conducting the financial statement audit, the auditor shall obtain an understanding of the components of internal control and assess the level of control risk relevant to the assertions embodied in the classes of transactions, account balances, and disclosure components of the financial statements. Such controls include relevant EDP general and application controls.

The OCFO produces the consolidated financial statements for the Department of Labor. The OCFO has implemented a centralized core accounting system called the Department of Labor Accounting and Related Systems (DOLAR$). DOLAR$ is comprised of the core system with feeder systems and subsystems providing additional data for processing. These feeder systems provide data from agencies managing their own financial data and other Federal agencies. The subsystem of DOLAR$ includes Accounts Payable, Accounts Receivable, Travel, etc.

Objective, Scope and Methodology

The Office of Inspector General (OIG) conducted a review of the automated controls over the Department of Labor Accounting and Related Systems (DOLAR$) application. The objective of our work was to review the critical application controls of the DOLAR$ application, in an effort to minimize the Department's risk associated with DOLAR$. The objective did not include rendering an opinion on the overall internal controls of DOLAR$.

We performed this review during the period of February 19, 2001 to April 6, 2001. Our testing covered those controls directly associated with the automated DOLAR$ application. We did not test any manual accounting controls that could potentially mitigate or impact the risks associated with weaknesses in the automated system control structure.

The application control review was developed and the controls tested were assessed using Federal guidance and criteria, consisting of:

- DOL's Computer Security Handbook
- National Institute of Standards and Technology Special Publication 800-18 *Guide for Developing Security Plan for Information Technology Systems*
- National Institute of Standards and Technology 800-12: *An Introduction to Computer Security*
- National Institute of Standards and Technology SP 800-14 *Generally Accepted Principles and Practices for Securing Information Technology Systems*
- OMB Circular A-130, *Appendix III*
- National Institute of Standards and Technology *FIPS PUB 73, Guidelines for Security of Computer Applications*
- National Institute of Standards and Technology, FIPS PUB 112 *Password Usage*

Our work was performed in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States.

We created data flow diagrams (DFDs) for the Core, Accounts Payable and Accounts Receivable subsystem of DOLAR$ during the Control Identification and Preliminary Assessment Phase. These DFDs documented the critical processes and location of key computer-related controls. We used this information to create a matrix for testing and evaluating the specific controls identified.

We conducted testing in five control categories: (1) Access, (2) Input, (3) Processing, (4) Rejection, and (5) Output. The following provides a brief description of the work completed.

Access Controls

Access controls testing assessed how security was implemented at the application level in the areas of user access, general security features of DOLAR$, and segregation of duties. There is a total population of 620 DOLAR$ users, with approximately 420 users having read-only access and 200 users with update capabilities. We conducted some of the tests using the whole population of 620 users. We conducted other tests using a judgmental selection of 23 users to determine whether or not user access was appropriately granted based upon the "least privileged" concept

Input Controls

Input controls testing assessed edits and validations to determine the accuracy, completeness, and integrity of data being entered via online, batch, and/or interface files from other systems. We conducted testing on a selection of critical fields having a financial statement impact or high volume of transactions processed.

Processing and Rejection Controls

Processing and rejection controls were assessed to determine whether application controls in place over the processing of data would preclude or detect the erroneous or unauthorized addition, removal, or alteration of data during processing. In addition, we performed testing of processing controls to determine whether selected transactions impacting critical management reports were accurately and completely recorded and posted to the general ledger. Process control testing involved mapping transactions, both on-line and batch, through the application from initial input, processing, and output. Mapping is the process of determining that selected transactions post to the correct general ledger accounts and critical management reports accurately and completely reflect the information that is input and processed by the application.

On-line transaction testing was based upon a selection of screens or functions deemed critical by the OIG. These screens/functions included the Accounts Payable subsystem and critical Core screens (i.e., Generic Entry, Fund Receipt). Our determination of testing was based on the frequency and dollar amount of DOLAR$ batches received or created. The following batches were tested:

- PMS / HHS (Payment Maintenance System / Health and Human Services)
- ESA / FECA (Federal Employment Compensation Act)
- Payroll
- UTF / Treasury (Unemployment Trust Fund)

Output Controls

We assessed output controls to determine whether information processed by DOLAR$ was accurately captured on critical management reports.

Computer Assisted Audit Techniques (CAAT)

The CAAT testing was based on a file from DOLAR$ containing over 2.2 million transactions that were posted between October 1, 2000 and February 28, 2001. The CAAT testing focused on the following control areas:

Access Controls

- User IDs with posted transactions to DOLAR$ during the 5-month period
- Users with update access without posted transactions to DOLAR$ during the 5-month period

Input Controls

- Required fields were populated
- Fields consisted only of valid entries

Processing Controls

- Cut-off controls prevented transactions from posting in prior or future periods
- Transaction codes were only posting to the designated general ledger accounts (this test was performed on selected general ledger accounts and transaction codes).

Findings and Recommendations

1. Security management of DOLAR$ is weakened by a lack of policies and procedures and effective monitoring and maintenance of user accounts.

A. User Account Management

We reviewed User Account Management and found that security management was ineffective in controlling user access rights to the DOLAR$ application. Specifically, we found that:

- policies and procedures for granting and certifying user access rights have not been maintained (Note: this issue was identified and reported as part of the general controls review);
- unrestricted access to critical screens (i.e., Generic Entry, Vendor Maintenance) had been granted to several users;
- users maintain current and active DOLAR$ processing capabilities, but have not recently posted transactions; management level users were able to verify their own access recertification forms;
- several users were assigned to more than one user ID;
- the Security Officer's user ID and password is shared between the security and backup security officers (Note: the backup security officer also maintained a second user ID); and
- the Security Officer's user ID was used to process business transactions.

Without effective controls over the establishment and maintenance of well-defined user classes, access control lists, and assignment of access based upon a business need, users may receive processing capabilities for both initiating and approving transactions, circumventing the checks and balances of the system. In addition, these weaknesses could potentially compromise the financial integrity of the general ledger.

Recommendations

We recommend that the Chief Financial Officer (CFO):

1. Ensure that the OCFO's user access policy and procedures are in compliance with the Computer Security Handbook and that the OCFO's System Security Plan (SSP) for DOLAR$ contains sufficient policies and procedures governing the authorization, modification, removal,

monitoring of access based on the concept of "least privileged," and emergency access. In addition, the DOLAR$ SSP should include specific technical standards (security settings, critical system configuration, etc.). (Note: this is a modified recommendation from the general controls review.)

2. Create user classes (profiles) based on the user's job functions and responsibilities. User management and security administration should conduct a review to define a limited number of user classes, based on job title. For each position, the responsibilities, and thus the function codes, should be determined using the "least privileged" concept. (Note: user classes and function codes may need to be created, modified or deleted.) Once the new "user access matrix" has been created, it should be approved by the appropriate level of user management and security administration and included in the SSP. Additionally, all current users should be mapped to the appropriate new user class. See below diagram for example of "user access matrix."

Example User Access Matrix

Region/ Field Office	User Classes (Profiles)	Job Description/ DOLAR$ Responsibilities	Function Code	Assigned Staff
Denver, CO	Accounts Payable Clerk 1	Invoice Receipt Invoice Processing Voucher Payment	IR IP VP	John S. Mary D.
	Accounts Payable Supervisor	Vendor Maintenance	VM	Bob D. Sue B.
Washington, DC	Accounts Payable Clerk 1	Invoice Receipt Invoice Processing Voucher Payment XXXXX WWWW	IR IP VP XX WW	Kevin K. Regina R.

3. Address the recertification process in the DOLAR$ draft SSP and ensure the SSP includes the following:
   - providing guidance to the manager on how to complete the recertification forms;
   - defining the frequency of the recertification (at least annually);
   - identifying the signing authorities;
   - determining user statistics (types of transactions users process, date the user ID was last used, interval of time between last password change, etc.);
   - identifying and removing duplicate user IDs; and
   - defining the Security Officer's and the back-up Security Officer's roles and responsibilities to clearly restrict the Security Officers' ability to

perform business transactions. Unique user IDs and passwords should be established for accountability between the two positions, eliminating the sharing of the Security Officer's user ID.

Management's Response

The DOLAR$ SSP will be updated to incorporate: (1) policy and procedures for granting and certifying user access rights; (2) guidelines for monitoring and managing inactive IDs; and (3) guidelines for issuing multiple user IDs to individual users.

The OCFO has completed a review of the small percentage of users with access to the Generic Entry and the Vendor Maintenance screens and has determined that their level of access is consistent with their level of financial authority and responsibility, and is reinforced by the application of TC-Rules appropriate to each individual position. Access to these screens is greatly limited. To do away with this capability would impede the DOL's ability to carry out efficiently and effectively its financial management functions.

The observation that "several" users were assigned multiple user IDs is both unclear and inaccurate. Because of dual-period processing, DOLAR$ requires that user IDs be set up for the accounts payable portion of a user's access though a user can not also sign into DOLAR$ with that "second" user ID. Its use is strictly for posting from the accounts payable batch process. During the review period, there was only one legitimate update-capable user who had two separate user IDs. The OCFO can provide more detail on that user's need if necessary.

The recertification process will be modified to preclude management level users' ability to verify their own recertification forms.

The Security Officer and the Back-up Security Officer do not maintain a second security ID. The Security Officer's ID had been but is no longer used to process business transactions. To accommodate the system requirement that the Security Officer and the Back-up Security Officer have joint use of the security user ID, the DOLAR$ SSP will include procedures that require the control and modification of the Security Officer's user ID and password.

The OCFO disagrees with the recommendation to implement a new "user access matrix" using the "least privileged concept." The OCFO believes that the DOLAR$ TC-Rule provides adequate granularity. The TC-Rule defines each user's access to each DOLAR$ screen by Action Code, Document Type and Transaction Code. The TC-Rule permits a customized approach to system access

and internal controls based on a Servicing Finance Office's needs, staffing, and functions.

OIG's Conclusion

We concur with the OCFO's planned action to update the SSP to better address security.

We disagree with the OCFO that the current system of assigning authority provides adequate granularity. The appropriate use of user classes (profiles) helps to minimize the risks in user and access management. Additionally, during our review OCFO personnel noted that over the years, different security officers have "created additional user classes out of convenience and not necessity."

We concur with the OCFO's planned action to modify the recertification process and update the SSP to include the new process and procedures.

We agree with the OCFO that the Security Officer and the Back-Up Security Officer are sharing one user ID to perform this function. However, it is noted that the OCFO will be addressing this weakness with additional policies and procedures in the SSP. The OIG will review the policies and procedures when they are developed to evaluate whether this action will mitigate the identified weakness.

The three recommendations are all unresolved. The actions noted for Recommendation 1, regarding the update of User Access in the SSP, will resolve the recommendation; however, the CFO needs to provide a timeframe for implementation. Resolution of Recommendation 2, regarding the correct use of user classes (profiles) for assigning access, will require the CFO to implement the user class security feature of DOLAR$. The actions notes for Recommendation 3, regarding the recertification process, will resolve the recommendation; however, the CFO needs to provide a timeframe for implementation.

B. Technical Controls

We found that technical controls, designed to automatically control password maintenance were not utilized and do not provide base-line security over the DOLAR$ general ledger. Specifically, we found that:

- Controls designed to ensure that users were changing their passwords on a regular interval were not effective. Our testing revealed that 36 percent of the

DOLAR$ users had not changed their default passwords or were not changing their passwords regularly. (Note: the DOLAR$ applications operates on an IDMS database that does not force password change intervals. This issue was documented as part of the general controls review.)

- The default password is easy to guess and widely known among the user community.
- Passwords associated with sensitive user IDs (i.e., Chief System Administrator, Security Officer) have not been regularly changed.

Unauthorized users could access the system using a default password. System security passwords that are not adequately protected or monitored can be used to circumvent controls and access critical processing and system management capabilities. Unauthorized access could compromise the integrity of the system and the financial data processing.

Recommendations

We recommend that the CFO:

4. Continue efforts to implement automated password parameter features (e.g., password expiration intervals, stronger password composition, lockout features, etc.). In addition, until an automated feature can be found to strengthen password controls, the manual control currently performed by the security group should be enhanced and enforced.

5. Create and implement to all DOLAR$ users, a password policy, that complies with the CIO's Computer Security Handbook. The policy should, at a minimum:
   - state the password composition rules and password change interval (every 30 days);
   - inform the user community that reviews will be conducted to enforce the policy; and
   - clearly state that noncompliance with the policy will be considered a violation resulting in the inactivation of the user ID.

The DOLAR$ security group should conduct monthly reviews to enforce the policy. Noncompliance with the policy should be considered a violation, documented as such and result in inactivation of the user ID. In addition, the OCFO should research a mechanism of sending global messages to remind users logging onto the system to change their passwords regularly.

Management's Response

The OCFO will implement the automated password parameter features as planned. Until then, the OCFO will continue to improve upon methods of: (1) informing individuals with user IDs of the password composition rules; (2) reviewing monthly reports that reflect the frequency of changes to passwords; and (3) deactivating those user IDs belonging to users who fail to change their default password.

OIG's Conclusion

We concur with the OCFO's planned action to implement automated password features. With the lack of the automated features, we urge the OCFO to quickly implement the recommendation to enhance and enforce the current manual controls for password maintenance. Recommendation 4 is unresolved; resolution is dependant on the OCFO providing the timeframe for implementation of an automated password control feature. Recommendation 5 is unresolved pending a plan to implement the stronger manuals controls outlined by the OCFO in its response.

2. The accuracy, completeness and integrity of the information processed and stored by the DOLAR$ application is weakened by inadequate application functionality.

A. Application Audit Trails

We found two instances of ineffective audit trails for the DOLAR$ application. First, the edit history for all transactions maintains only the prior editor's user ID. Without an adequate audit trail, a user could potentially validate a payable entered by that user. This increases the risk that improperly authorized transactions could be processed and paid. The accountability over changes are diminished when only one user ID is associated with a transaction.

Second, DOLAR$ does not maintain a history of the changes performed using the "TLCC" transaction code. This code allows changes to specific fields (i.e., ALC, schedule number, and invoice number) already posted. The changes overwrite the original record and create two identical records.

The DOLAR$ system limitation of only maintaining a limited audit trail could minimize DOL's ability to identify changes made to processed transactions. This weakness becomes more significant when considered with the weaknesses

associated with user account management and vendor table maintenance and excessive access.

Recommendations

We recommend the CFO:

6. Implement additional controls to capture at least two user IDs for critical processing functions to force segregation of duties.

7. Disable the “TLCC” transaction code (TC).

8. Perform a review of all TCs to ensure a business need exists and to ensure that the TCs do not expose the Department to potential security vulnerabilities.

Management’s Response

The statement that "DOLAR$ maintains only the prior editor's user ID,” while accurate for invoice processing, is not accurate for DOLAR$ transaction processing. DOLAR$ only requires a single user ID for core transactions as changes to those transactions are not allowed now that the TLCC has been removed. The OCFO will review the invoice processing to determine how best to maintain the initial user (control number identifier) as well as a second user who might modify the record.

The OCFO will establish appropriate internal controls necessary to address OIG’s recommendation to implement additional controls to capture at least two user IDs for critical processing functions, approval of payments, etc., to force segregation of duties.

The OCFO believes that the auditors failed to test the "Transaction Correct (TLCC) code. While changes via the TLCC code are not identifiable to the normal user, the information is maintained on the 650-byte transaction ledger record and can be accessed by an on-line query (OLQ). Nevertheless, the OCFO has disabled this process and requires the user to reverse the incorrect entry and to re-post the corrected entry.

The audit report does not include an associated finding that warrants the third recommendation to perform a review of all TCs. What is the basis for the recommendation?

OIG's Conclusion

The actions taken on our recommendation to remove the "TLCC" transaction code has partially resolved the recommendation to implement controls to capture additional information on critical processing and payment functions. However, the OCFO still needs to establish controls to capture information to enforce segregation of duties and ensure accountability. Recommendation 6 is unresolved. To resolve this issue, the OCFO needs to provide a plan including timeframes for establishing and implementing the controls.

We agree with the action of the OCFO to disable the "TLCC" transaction code. Recommendation 7 is resolved and open. Closure is dependent on the results of testing to be conducted as part of the FY 2002 financial statement work. We have asked the financial statement auditors to provide information on the use of the "TLCC" transaction code.

We disagree with the OCFO about the need to perform a review of all TCs for business need and security. The "TLCC" transaction code allowed changes to records circumventing controls; the OCFO should have an interest in ensuring that other TCs do not open up the Department for additional unnecessary risks. Recommendation 8 is unresolved. In order to resolve this recommendation, the OCFO needs to address this as a security risk and take appropriate measures to ensure that this risk is minimized to the greatest extent possible by reviewing the transaction codes.

B. Vendor Maintenance

We found that a large percentage (50%) of DOLAR$ users have vendor update processing capability through the Vendor Maintenance Table. In addition to these users, the DOLAR$ application allows users with processing capability in the A/P subsystem to also add new or change existing vendor information. Inadequate controls over the vendor table increase the risk of duplicate payments, payments to unauthorized vendors or persons, and inactivating authorized vendors leading to delays in payments. In addition, vendor table information can be added or modified without the controls of the Vendor Maintenance Table. The ability to enter vendor information outside of the Vendor Maintenance Table increases the difficulty of managing authorized vendors.

Recommendations

We recommend the CFO:

9. Immediately conduct a review of all individuals having access to the Vendor Maintenance Table. The ability to add, modify, and/or delete information from the vendor maintenance table should be considered a critical function within DOLAR$ and access should be restricted to a tightly controlled group.

10. Restrict the ability to update the vender table from the A/P subsystem.

11. Immediately conduct a review of the vendor table to identify and remove duplicate, inactive, and unauthorized vendors. Once completed, the OCFO should conduct periodic reviews of the vendor maintenance table.

Management's Response

The OCFO disagrees with two findings in this area. While fifty percent of DOLAR$ user have access to the critical screen in the database, a far lower percentage of those users have update capabilities on that screen. DOLAR$ TC-Rule limits that ability. Secondly, while a vendor record can be created on the Invoice Register screen, that vendor is created as "inactive" and must be activated by a user that has update access to the Vendor Maintenance screen before an invoice is processed for payment. We see no "weaknesses" in that process.

The OCFO has been and will continue to (1) review the vendor table to identify and remove duplicate vendors and (2) annually archive inactive vendors.

The OCFO has completed a review of the current users that have update capability to the Vendor Maintenance Table. As a result of this review, it was determined that this access by a limited number of users is required to accommodate the business need of each of DOL's servicing finance offices. The OCFO will establish the appropriate internal controls necessary to resolve this issue.

OIG's Conclusion

We disagree with the OCFO that a limited number of users had access to the vendor maintenance function. Our review showed that over 100 users had "Update" capability for the Vendor Maintenance Table. The OIG also maintains

that this "limited number" of users required to accommodate the business need is excessive and increases the risk of fraudulent payments. Recommendation 9 is unresolved. To resolve this recommendation, the OCFO needs to provide a detailed risk assessment defining the business need of the "limited number."

We disagree with the OCFO's position that the current ability to update the vendor table from the A/P subsystem is not a weakness. The OIG understands that when a vendor is created in the Invoice register screen, the new vendor is placed "inactive." However, the controls implemented in the Vendor Maintenance Table are effectively bypassed when not created using the Vendor Maintenance Screen, thus increasing the risk that improper payments could be issued and increasing the difficulty in managing the vendor table. Recommendation 10 is unresolved. To resolve this recommendation, the OCFO needs to develop controls to limit vendor creation outside of the Vendor Maintenance process.

The OCFO has stated "The OCFO has been and will continue to (1) review the vendor table to identify and remove duplicate vendors and (2) annually archive inactive vendors." Documentation or information has never been presented to validate this assertion. Recommendation 11 is unresolved. To resolve this recommendation the OCFO needs to provide documentation that demonstrates the reviews have occurred.

C. Prior Month Posting Observation

We found that user and system flags regulating prior period postings in DOLAR$ are not adequately controlling user capabilities. Users are able to post prior month transactions (excluding cash) if the system flag in the DOLAR$ Manager Table is set to Y (es) (allowing prior month transactions), regardless of whether or not the user's flag is set to Yes or No. Therefore, any user can post to a prior month when the prior period flag is set to Y.

Unauthorized users may post a transaction to a prior month, potentially causing accounting errors and impacting the integrity of financial reporting.

The prior month flag is functioning as designed by management. Although we have concerns over the ability of unauthorized users to post erroneous prior month transactions, due to the financial accounting impact of this observation, we have referred this issue to OIG's financial auditors for further review.

Management's Response

The OCFO has revised its dual-month processing capabilities to ensure that only those users that have the appropriate authority are allowed to post against the prior accounting period. The prior-month authority now mirrors the system's prior-year authority.

OIG's Conclusion

The OIG has disclosed the information to the independent financial auditors for review. The OIG has provided the Management's response to the independent financial auditors as well. As a part of this report, the observation is closed and will not be tracked.

D. Dollar Amount of Transactions

We found that controls regulating the dollar amount that can be entered for a transaction are not adequate. The "Amount" field allows transactions to be entered with a dollar amount as high as $9,999,999,999.99. This control affects any transaction processed in DOLAR$ on any screen, notably the generic entry screen. In addition, our tests show that nearly all transactions are for amounts less than $25,000, indicating that not all users need the ability to input transactions with high dollar amounts.

The lack of control on transaction amounts increases the risk to DOL that: (1) an individual wanting to commit fraud could misdirect a considerable amount of funding using only one transaction; and (2) a user could erroneously enter a high dollar amount impacting the integrity of the transaction and the associated financial data supporting the financial statements.

The following mitigating controls do exist to reduce the effects of the condition; however, they alone do not provide sufficient control.

- A transaction cannot be processed for any amount greater than what is available to be spent via DOLAR$ Fund Control.
- A user other than the one that processed the transaction must verify all accounts payable transactions prior to disbursement.

Recommendation

We recommend that the CFO:

12. Perform an assessment regarding how the users across the Department use the amount field in DOLAR$ and determine and implement a reasonable limit on this field.

Management's Response

OCFO has determined that limiting the amount field would hinder DOL's ability to process timely and efficiently payments and transactions. In addition to the mitigating controls referenced in the finding, the OCFO has other controls, such as (1) daily monitoring of the status of funds and (2) daily review of the suspense file, including contacting the appropriate servicing finance office(s) to determine the nature of items on the file.

OIG's Conclusion

We do not concur that implementing such controls would necessarily hinder DOL's ability to process payments and transactions timely and efficiently. Two alternative methods of accomplishing this control objective include the creation of a daily exception report produced for supervisory approval or the requiring of supervisory approval prior to processing of the transaction. Either of these or both would provide reasonable assurance that the transaction was accurate and authorized, without hindering DOL's ability to process payment and transactions in a timely and efficiently manner. Recommendation 12 is unresolved. To resolve this recommendation, the OCFO needs to provide the OIG with a formal risk assessment showing the OCFO has reviewed the risk and accepts it or implements the recommendation.

Acronyms

A/P	Accounts Payable
CAAT	Computer Assisted Auditing Techniques
CFO	Chief Financial Officer
CIO	Chief Information Officer
DFD	Data Flow Diagrams
DOL	Department of Labor
DOLAR$	Department of Labor Accounting and Related Systems
ESA/FECA	ESA's Federal Employees' Compensation Act
NIST	National Institute of Standards and Technology
OCFO	Office of the Chief Financial Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
PMS/HHS	Payment Maintenance System/Health and Human Services
SSP	System Security Plan
TC	Transaction Code
UTF	Unemployment Trust Fund