



Audit Report



OIG-05-017

Management Letter For Fiscal Year 2004 Audit of the
Department of the Treasury's Financial Statements

December 14, 2004

Office of
Inspector General

Department of the Treasury



OFFICE OF
INSPECTOR GENERAL

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

December 14, 2004

MEMORANDUM FOR BARRY HUDSON
ACTING CHIEF FINANCIAL OFFICER

FROM: William H. Pugh *William H. Pugh*
Deputy Assistant Inspector General
for Financial Management and Information
Technology Audits

SUBJECT: Management Letter for Fiscal Year 2004 Audit of
the Department of the Treasury's Financial
Statements

I am pleased to transmit the attached management letter in support of the audited Department of the Treasury's (Department) Fiscal Year (FY) 2004 financial statements. We contracted with the independent certified public accounting firm of KPMG LLP to audit the Department's financial statements for FY 2004. The contract required that the audit be performed in accordance with generally accepted Government auditing standards; Office of Management and Budget Bulletin No. 01-02, Audit Requirements for Federal Financial Statements, and the *GAO/PCIE* Financial Audit Manual.

As part of its audit, KPMG LLP issued and is responsible for the accompanying management letter that discusses certain matters involving internal control over financial reporting and its operations that were identified during the audit which were not required to be included in the audit report.

In connection with the contract, we reviewed KPMG LLP's letter and related documentation and inquired of its representatives. Our review disclosed no instances where KPMG LLP did not comply, in all material respects, with generally accepted Government auditing standards.

Should you have any questions, please contact me at
(202) 927-5400, or a member of your staff may contact
Mike Fitzgerald, Director, Financial Audits at (202) 927-5789.

Attachment

cc: Dennis S. Schindel
Acting Inspector General

Marla A. Freedman
Assistant Inspector General For Audit



KPMG LLP
2001 M Street, NW
Washington, DC 20036

Inspector General
U.S. Department of the Treasury

We have audited the consolidated financial statements of the U. S. Department of the Treasury (Department) as of and for the year ended September 30, 2004, and have issued our report thereon dated November 12, 2004. Our report indicated that we did not audit the amounts included in the consolidated financial statements related to the Internal Revenue Service (IRS), a component entity of the Department, or the gold and silver reserves of the U.S. Government. In planning and performing our audit of the consolidated financial statements, we considered the Department's internal control over financial reporting in order to determine our auditing procedures for the purpose of expressing an opinion on the consolidated financial statements, and not to provide assurance on internal control over financial reporting.

During our FY 2004 audit of the Department's consolidated financial statements, we and the other auditors noted certain matters involving internal control over financial reporting and its operations that we considered to be reportable conditions under standards established by the American Institute of Certified Public Accountants. Reportable conditions are matters coming to our attention relating to significant deficiencies in the design or operation of internal control that, in our judgment, could adversely affect the Department's ability to record, process, summarize, and report financial data consistent with the assertions of management in the consolidated financial statements. Our consideration of internal control over financial reporting would not necessarily disclose all matters in internal control that might be reportable conditions. In our *Independent Auditors' Report* dated November 12, 2004, we reported the following matters involving internal control over financial reporting and its operation that we and the other auditors considered to be reportable conditions:

- Financial Management and Reporting at the IRS Needs Improvement
- Electronic Data Processing Controls Over Financial Systems at the Financial Management Service Should Be Strengthened

The reportable condition related to financial management and reporting at the IRS noted above is considered to be a material weakness. Detailed findings and recommendations to address the above reportable conditions are not repeated within this document.

Our audit procedures were designed primarily to enable us to form an opinion, based on our audit and the reports of the other auditors, on the Department's consolidated financial statements and, therefore, may not bring to light all weaknesses in policies or procedures that exist. However, we take this opportunity to share our knowledge of the Department, gained during our work, to make comments and suggestions that we hope can be useful to you.



Although not considered reportable conditions, we noted certain matters involving internal control and other operational matters that are presented in the attachment for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of Department management, are intended to improve the Department's internal control or result in other operating efficiencies. The matters presented in this letter do not include any internal control or operational matters that may have been presented to the management of the Department's operating bureaus that were separately audited by other auditors. Two prior year comments with continuing relevance have been updated and identified in the attachment as "repeat comments." The other prior year comment related to the process for preparation of the Department's Performance and Accountability Report (PAR) has not been repeated, as we believe sufficient improvement has been made to consider this matter closed. We have not considered the Department's internal control since the date of our report.

We appreciate the courteous and professional assistance that Department personnel extended to us during our audit. We would be pleased to discuss these comments and recommendations with you at any time.

This report is intended solely for the information and use of the U. S. Department of the Treasury and its Office of Inspector General and is not intended to be and should not be used by anyone other than these specified parties.

KPMG LLP

December 13, 2004

U.S. Department of the Treasury
Letter to Management on Internal Control
Fiscal Year Ended September 30, 2004

I. Financial Reporting Standards for Department Component Entities Should be Consistent (Repeat Comment)

The Department's consolidated financial statements are prepared in conformity with accounting principles prescribed by the Federal Accounting Standards Advisory Board (FASAB), the accounting standards-setting body for the Federal Government, as recognized by the American Institute of Certified Public Accountants in October 1999. However, certain Department component entities prepare their financial statements in accordance with accounting standards prescribed by the Financial Accounting Standards Board (FASB), the private sector standards-setting body, since the FASAB has allowed entities that issued financial statements prior to October 1999 using FASB accounting principles to continue to do so. These entities include the Bureau of Engraving and Printing (BEP), the United States Mint (Mint), the Office of Thrift Supervision (OTS), the Exchange Stabilization Fund (ESF), the Federal Financing Bank (FFB), and the Community Development Financial Institutions Fund (CDFI).

The use of a combination of generally accepted accounting principles (GAAP) by the Department and its component entities complicates the preparation of the Department's consolidated financial statements since, additional information required for Federal GAAP reporting must be developed, mapped and submitted to the Department's data warehouse by component entities, and reviewed for compliance with federal GAAP and overall reasonableness by Departmental accounting management. In addition, the separately issued financial statements of the component entities using FASB accounting principles do not adequately portray the importance of the budgetary process as it relates to federal entities. That is, the concept of "presents fairly" for these entities is incomplete as it relates to the significant budgetary disclosures required by federal GAAP.

Private sector GAAP does not contemplate budgetary reporting and therefore components using this basis of accounting do not prepare statements of budgetary resources or statements of financing, although these statements are an integral part of the Department's consolidated financial statements, and must be prepared regardless of whether the component receives appropriations from the U.S. Government's general fund or not. Moreover, information reported in the Department's SBR must be reconciled to enacted amounts in the President's Budget and disclosed in the footnotes to the Department's consolidated financial statements. Considerable additional preparation and audit steps are required to develop and report this data at the Department level for components using private sector GAAP.

Additionally, private sector GAAP does not provide sufficient information regarding the costs of programs and activities. The statement of net cost required by Federal GAAP requires that costs and offsetting earned revenues be presented by responsibility segments, with net costs identified for each of the segments, in order to provide more meaningful information to evaluate the operating results of major activities.

Further, inconsistencies exist in how certain costs are reported by entities using private sector GAAP. For example, Federal GAAP requires that non-reimbursed costs paid by the Office of Personnel Management for retirement plans be recognized by the receiving entity as an imputed cost in order to report the full cost of operations. Since private sector GAAP does not provide guidance for the reporting of imputed costs, these costs are being reported inconsistently, or not at all, by the Department's component entities.

Finally, private sector GAAP does not require management's discussion and analysis (MD&A) of the information presented in the annual report. The MD&A is one of the most valuable aspects of an annual financial report, since it provides management's assessment of key trends, fluctuations, and unusual items. It should also link financial and performance information to provide meaningful analysis of the cost benefit relationships of program accomplishments. Several of the Department's component entities using private sector GAAP do not present an MD&A in their annual reports.

The continued use of private sector GAAP by certain Department component entities decreases the usefulness of information reported by these entities for users of federal financial statements. In order to strengthen and standardize financial accounting and reporting throughout the Department, all component entities should be required to prepare their financial statements in accordance with Federal GAAP, unless statutorily required to report on a different basis of accounting.

Recommendation:

We recommend that the Department research and determine whether component reporting entities reporting on a basis other than Federal GAAP are required to do so by statute. We further recommend that (1) all reporting entities within the Department prepare their financial statements in accordance with Federal GAAP, unless statutorily required to report in accordance with a different basis of accounting, and (2) entities that are statutorily required to report on a basis of accounting other than Federal GAAP provide supplemental information in their annual reports that meets the reporting requirements of Federal GAAP, to include an MD&A.

Management Response:

The Department requires that all bureaus comply with the United States Standard General Ledger (USSGL), which is used for Federal sector GAAP. The USSGL balances transmitted by the bureaus to the Department's centralized database are appropriately mapped to reflect transactions on a Federal GAAP basis in the Department's consolidated financial statements. No errors resulting from conversion from private sector GAAP were noted in the Department's FY 2004 or 2003 consolidated financial statements. The Department will continue to explore, with the relevant bureaus, the need to produce their standalone financial statements on a Federal sector GAAP basis.

In April 2004, the OIG requested that FASAB consider requiring Federal GAAP for the general purpose financial statements of Federal entities, unless there is a statutory or regulatory requirement to report on a different basis. A response has not been received to date.

**II. Analysis of Financial Reports at the Department Level Should Be Improved.
(Repeat Comment)**

In conducting our audit of the Department's FY2004 PAR, we noted that Department management was not always able to provide explanations for variances or unusual relationships in the interim and year-end financial data compiled for the Department as a whole. We were often informed that reasons for variances were not readily available because the variances originated at the bureau level and that the Department was not knowledgeable enough to explain the variance to us. However, when pressed for information, the Department was able to obtain the information from the bureaus to satisfy our questions.

We understand that the Department uses its 3-Day Close Data Quality Scorecard to assess the quality of monthly data submitted by its bureaus. This scorecard generally serves as a data input check to ensure that, for certain critical accounts, balances are submitted, are properly recorded as debits or credits, properly coded, and reflect periodic changes. This provides a useful mechanical check over data submissions,

however, it does not provide an analysis of the reasonableness of the balances, nor explanations for unusual variances. The data quality checks need to be supplemented by more in-depth analytical review procedures to evaluate the overall reasonableness of the data on a timely basis.

Analytical review procedures should be applied to examine relationships between financial data and relevant non-financial information, such as program performance data. Such analysis is the most meaningful, since it provides information to evaluate efficiency and cost effectiveness in achieving program and operational objectives.

The Department should oversee and monitor analytical reviews performed by its component entities, and perform additional reviews and analyses of the consolidated data to ensure the quality and reliability of the financial reporting of the Department as a whole. These additional controls over the interim and year-end reporting processes should result in more reliable and meaningful financial information being available to users of the Department's financial data throughout the year.

Recommendation:

We recommend that interim and year-end analytical review procedures be strengthened to include identification and follow-up with appropriate Departmental and component entity level management of significant variances and unusual financial and performance measure relationships as an integral part of the financial reporting process. The results of the analyses should be documented in brief narratives accompanying the financial reports.

Management Response:

The Department prepared analytical reviews of its FY 2004 interim and final financial statements, including explaining any unusual balances and significant fluctuations. Certain bureaus also submitted analytical reviews during FY 2004. The Department plans to formalize its procedures and will work with the bureaus to provide formalized procedures that complement the Department's.

III. Fund Balance With Treasury Reconciliations Should Be Prepared on a Consistent Basis

Observation:

Fund Balance with Treasury (FBWT) reconciliations were either not prepared timely or not prepared at all for the funds managed by Treasury's Departmental Offices (DO). In addition, reconciliation differences were not addressed and resolved timely throughout the year. For example, as of September 30, 2004, no actions had been taken to resolve some of the differences that had been identified between the FMS 224, *Statement of Transactions* and FMS 6652, *Statement of Differences* since December 2003, and the FMS 6653, *Undisbursed Appropriation Account Ledger* reconciliation had not been prepared for certain funds in the latter part of fiscal year (FY) 2004 (e.g., funds 20X4501 and 2040101). Differences identified at year-end between the respective general ledger balances applicable to certain managed funds and the FMS 6653 ranged from \$130 to \$691,909, some of which resulted from the lack of regular monthly reconciliations being prepared during the year.

DO is responsible for the preparation of FBWT reconciliations and associated procedures for 25 funds (DO managed funds). DO reports the monthly disbursements and receipt transactions for DO managed funds on a consolidated FMS 224. Accordingly, the FMS 6652 reconciliation is also prepared on a consolidated basis. The FMS 6653 and the FMS 6655 are summary balance reports and the reconciliations for these are prepared individually for each of the DO managed funds by various DO personnel.

Treasury Financial Manual (TFM) - Part 2 – Chapter 5100, *Reconciling Fund Balance with Treasury Accounts*, requires agencies to reconcile their FBWT accounts on a regular and recurring basis to ensure the integrity and accuracy of their internal and Government-wide financial report data.

Additionally, the TFM requires that agencies use entry logs or other appropriate schedules for all verified collection, disbursement, and Intergovernmental Payment and Collection (IPAC) transactions reported on their FMS 224s and posted to Standard General Ledger (SGL) 1010 account. At the end of each accounting month, an agency is required to verify that the amounts reflected on its supporting documentation agree with its postings to the SGL 1010 account.

To ensure the accuracy of the Government's overall receipt and disbursement activity, Treasury's Financial Management Service (FMS) compares the agencies' reporting with the transaction activity provided by Regional Finance Centers, Disbursing Offices, Federal Reserve Banks, and other depositories. This comparison validates monthly receipt and disbursement data and determines the accuracy of the U.S. Government's operating cash. FMS produces FMS 6652s to identify differences between deposit and disbursement data from the agencies and from other sources. Agencies are required to reconcile any identified differences returned to them on the FMS 6652 monthly.

We were informed that DO did not consistently prepare the required reconciliations because of the need to devote resources to other priorities within DO.

Unresolved differences between FMS and DO's records compromise the reliability of FBWT balances and related accounts and the Department's published financial reports. Failure to implement timely and effective reconciliation processes could:

- Increase the risks of fraud, waste, and mismanagement of funds;
- Affect the Department's ability to effectively monitor budget execution; and,
- Impair the Department's ability to accurately measure the full cost of its programs.

Recommendation:

We recommend that the Accounting Officer, Departmental Offices, Office of Financial Management:

- Ensure that the FBWT reconciliation procedures currently in existence are consistently followed;
- Require that disposition of all discrepancies identified during the monthly reconciliation process for all funds be made on a timely basis; and
- Establish procedures for management to monitor and review the reconciliation process.

Management Response:

The Office of Financial Management (OFM) transitioned to a new financial accounting system, Oracle Financials, a new financial reporting system, Discoverer, and a new electronic requisition and procurement system, PRISM, at the beginning of fiscal year 2004, on October 1, 2003. Since starting on the new systems, the Office of Financial Management has been experiencing difficulties and problems reconciling Fund Balance with Treasury (FBWT) and resolving outstanding statement of difference (SOD) items identified in the reconciliation process in a timely manner. When transitioning to any new systems, it can be reasonably expected that processing transaction errors will increase as a result of the staff's diminished experience entering recurring and routine transactions for accounts payable, accounts

receivable and journal entries. This was OFM's experience also. OFM staff found Oracle Financials tedious and less user friendly than the previous accounting system. The volume of errors increased in the first quarter of fiscal year 2004 in relation to prior years, but reduced each quarter thereafter as expected. As errors were identified, this necessitated correcting entries be processed to resolve the errors. These correcting entries can be complex and usually require a thorough understanding of the financial accounting system to achieve the desired posting. To ensure the accuracy of correcting entries, the accounting staff relies heavily on the reporting capabilities of the accounting system, in this case Discoverer, to provide reports that verify entries posted appropriately. Initially, we found that the reporting capabilities of Discoverer were inadequate and not comparable to our capabilities in the previous accounting system. Programming work has been ongoing throughout the year to refine and enhance the reporting capabilities of Discoverer to meet our needs and requirements.

Presently, we are following our established policies and procedures that have been proven effective in the past in reconciling FBWT and appropriately resolving outstanding statement of difference items in a timely manner. We have devoted additional resources and management continues to closely monitor progress and improve our performance in this area. OFM has a dedicated accounting staff member that presently oversees and coordinates the FBWT Treasury reconciliations and continually updates management on the progress and issues to date. We are confident that this finding will be resolved in the FY 2005 reporting period based on our progress to date, dedication of increased staff and resources, and our determination to work effectively with our cross-servicing agency to modify and enhance the new systems to work effectively.

IV. The Exchange Stabilization Fund Budgetary Accounting Methodology Should Be Clarified

Observation:

The Exchange Stabilization Fund (ESF) maintains a transaction-based accounting system for the federal proprietary SGL accounts, but does not have a transaction-based budgetary accounting system. Some of the ESF budgetary data reported in the Treasury Information Executive Repository (TIER) is misclassified or inaccurate, but has been left in TIER to force a fit with the Office of Management and Budget's (OMB) budgetary accounting definitions. For example, undelivered orders, SGL account 4801, has been reported in ESF's trial balance as \$14.1 billion since FY 2000. However, ESF does not report any undelivered orders in its Statement of Budgetary Resources (SBR) nor does it have any transactions that meet the OMB definition of undelivered orders. As a result, ESF's SBR must be prepared manually outside of TIER and outside of CFO Vision, the Department's financial reporting system that converts TIER data into its financial statements.

Additionally, ESF does not include a FBWT account in its financial statements. However, in order to pass the Federal Agencies' Centralized Trial-Balance System (FACTS II) edit checks, ESF must reclassify amounts from its cash and other monetary asset accounts to FBWT. In FY 2004, ESF reported to FMS' FACTS II, \$16.5 billion in FBWT. The Department also must erroneously report amounts in FBWT in its required monthly report, FMS 224, *Statement of Transactions*.

Further, ESF's reporting to OMB for purposes of comparison to the President's Budget is also inconsistent with ESF's audited financial reporting data and requires reconciliation each year.

OMB Circular No. A-11, Part IV requires non-appropriated funds, such as the ESF, (as well as appropriated funds) to be included in an agency's combined SBR. It also requires the SBR to be based on OMB budget terminology, definitions and guidance. In addition, OMB Circular No.

A-127, Section 7a, requires federal financial management systems to "... ensure consistent information is collected for similar transactions throughout the agency, ...and ensure consistent information is readily available and provided to internal managers at all levels within the organization." Section 7c states further, "Reports produced by the systems that provide financial information, whether used internally or externally, shall provide financial data that can be traced directly to the SGL accounts."

The Department has complied with OMB and other reporting requirements by adopting unique budgetary applications for ESF data, but has not requested OMB to provide guidance concerning how to properly account for ESF transactions for reporting purposes on the Statements of Budgetary Resources and Financing and in the President's Budget. While the Department requested FMS to resolve the requirement to report FBWT to meet FACTS II edits and other FMS reports as early as 2002, FMS has been unable to provide an automated solution to date. No approved model of budgetary transactions exists for ESF that would ensure consistent budgetary and proprietary data is readily available that can be traced directly to the SGL accounts.

As a result, the Department's budgetary financial data for ESF submitted on the FMS 224 and to FACTS II for Government-wide reporting purposes is inconsistent with its SBR, Statement of Financing, and with the information provided to OMB for the President's Budget.

Recommendation:

- We recommend the Department's Acting Chief Financial Officer:
- Obtain guidance from OMB concerning how to properly account for ESF transactions for reporting purposes on the Statements of Budgetary Resources and Financing, recognizing that standard federal budgetary definitions do not apply to ESF's investment portfolio fund;
- Explore with OMB alternative ways of providing meaningful, accurate, and consistent data on the fund in the President's Budget and how the information should be reported in the Department's and Government-wide financial statements; and
- Continue working with FMS to obtain a solution to the problem of having to misclassify ESF funds to FBWT in order to meet FACTS II edit checks and FMS reporting requirements.

Management Response:

Management generally agreed with our findings. Suggestions were offered regarding the recommendations to (1) increase the Government's flexibility in determining appropriate solution(s) to ESF budgetary reporting and (2) emphasize the need for continued efforts with FMS to provide a solution to the misclassification of funds in FBWT.

V. Segregation of Duties Related to TIER Should Be Strengthened

Observation:

TIER was modified in March 2002 to allow Treasury bureau users to upload to both the TIER repository and the TIER holding area. This presents a segregation of duties weakness because it is critical that the same user not be able to upload to both the TIER repository and the TIER holding area without having a second person verify and validate the data.

OMB Circular A-130, *Management of Federal Information Resources*, issued under the authority of the Computer Security Act of 1987 (superceded by the Federal Information Security Management Act (FISMA) in 2002), guides that Federal organizations should incorporate controls such as segregation of

duties and least privilege. In addition, FISMA requires that Federal agencies comply with the information security guidance issued by National Institute of Standards and Technology (NIST). NIST Special Publication 800-12, *Introduction to Computer Security*, states that segregation of duties is the process by which users' roles and responsibilities are divided so that a single individual cannot subvert a critical process. NIST Special Publication 800-12 also states that users should only be granted access to functions necessary to accomplish their assigned responsibilities - thereby helping to maintain the principle of least privilege.

In March 2002, the TIER_PROG role was expanded to include the ability to upload into the repository. Prior to this modification, Treasury bureau users would need to have the TIER_ACCT role to upload into the repository. The designers of TIER originally envisioned that two separate users from a bureau would upload data into the holding area and the repository. Instead, most bureaus had a single individual with both roles granted that performed the data upload. One of the original designers of TIER stated that the change was done to provide functionality and a streamlined process in assigning roles.

This lack of TIER segregation of duties may allow Treasury bureau users to upload different data into the holding area, than that uploaded into the repository without having a second user validate the data. This provides an opportunity for an individual to bypass an internal control, which could potentially impact the integrity and accuracy of Treasury's consolidated financial reporting efforts.

Recommendation:

We recommend the Acting Chief Financial Officer, in coordination with the Chief Information Officer:

- Separate the TIER_ACCT privilege of loading data into the repository from the TIER_PROG role.
- Establish and implement a written, formal Treasury policy that clearly communicates Treasury's Department-wide compensating controls for maintaining financial data integrity and accuracy, if a valid business need prohibits Treasury from enforcing the previously existing segregation of duties policy.

Management Response:

The Department agrees with the intent of the recommendation to improve the internal controls associated with the submission of financial data from the bureaus to TIER. However, it has operational concerns about requiring two different TIER users to enter the data into the Holding Area and the Repository. This can be a burden to the smaller bureaus that do not have the staffing to always support this segregation of duties. In addition, this would require an extensive systems change to ensure that the same user did not submit the data during a given month. The Department will review the existing procedures and controls followed by the bureaus and determine options to mitigate the data submission risks. Appropriate controls will be developed and implemented to reduce this potential risk.

VI. CFO Vision Access Controls Should Be Strengthened

Observation:

The Department's access controls related to CFO Vision software do not include a requirement that users must change their application passwords after any set period of time. However, Treasury's IT Security Program (TDP-85-01) requires that passwords expire every 90 days (Section 5-1, part 1G).

Passwords are the first line of defense for many IT systems. Passwords are a technical measure that prevent unauthorized persons (or unauthorized processes) from entering a computer system. By not requiring users

to change their passwords, the protection provided by the password degrades over time, thereby increasing the risk of unauthorized access to key data.

Recommendation:

We recommend that the Acting Chief Financial Officer, in coordination with the Chief Information Officer, ensure CFO Vision complies with Treasury IT Security Program Standards requiring passwords to be changed every 90 days.

Management Response:

Management concurs with the recommendation. On September 13, 2004, the Department modified the CFO Vision procedures to require users to change their passwords every 180 days. On October 14, 2004, CFO Vision was modified to change the password refresh cycle from 180 days to 90 days in compliance with the Department's policy.

VII. TIER Access Controls Should Be Strengthened

Observation:

The Department's current deployment of Windows XP has a feature that allows a user to save his or her identification and authentication information. When a user is accessing TIER via the login screen, a pop-up box appears, providing an option to a user to save his or her unique ID and password information. Therefore, when that individual logs into TIER the next time, the user would not be forced to enter his or her unique ID and password. This setting thereby bypasses the TIER identification and authentication control of having each user enter a unique ID and password each time they log in. Treasury administrators have not disabled this feature.

This Windows XP feature provides the ability to circumvent a previously designed application control in TIER. If a user utilizes this feature and that individual leaves his or her workstation unattended and is logged on to the network, prior to logging into TIER, it allows an unauthorized individual to log onto TIER without having to enter any identification and authentication information. Once this is accomplished, this unauthorized user has all the same rights and privileges of the authorized user. Depending on the user's access rights, this individual could cause considerable harm to the data.

OMB Circular A-130 states that agencies are required to establish controls to assure adequate security for all information processed, transmitted, or stored in Federal automated information systems. Technical and operational controls are necessary to support management controls. To be effective, all controls must interrelate. For example, authentication of individual users is an important management control, for which password protection is a technical control. However, password protection will only be effective if both a strong technology is employed, and it is managed to assure that it is used correctly.

Recommendation:

We recommend that the Acting Chief Financial Officer, in coordination with the Chief Information Officer, consider the following options to mitigate this control weakness:

- Issue written, formal policy related to saving user names and passwords for applications.
- Request administrators to disable this feature if the operating system allows such disabling.

- Have the TIER login sequence re-worked so that user authorization information is not entered through a Windows login box, but possibly through a web browser where user information cannot be saved.

Management Response:

The Department does not concur with the observation and recommendations because, in accordance with the Departmental Office's IT Policy Manual (based on TDP 85-01, Section 4.1.1), the storage of user passwords is permitted so long as they are encrypted for storage. While the Department recognizes some risk inherent in the storage of passwords, through the use of multiple levels of login procedures, it is willing to accept this level of risk.

Further, as part of the FARS Certification and Accreditation (C&A) (which includes TIER), the Rules of Behavior instruct users to "Never leave the workstation unattended without taking the necessary security precautions (e.g., password-protected screen savers, or completely logging off the system.)" Additionally, Department employees undergo background investigations upon employment and, in accordance with the C&A system, take the Department "systems security awareness training" before obtaining access to the system. As a result, the Department is confident that access controls are at an acceptable level of risk.

Auditor Comments:

While Treasury management does not concur with the finding and recommendations, it does agree with the basic facts presented. As such, we will continue to keep our recommendations open in order to validate management's representations above during the FY 2005 audit process.