GAO

Accountability * Integrity * Reliability

United States General Accounting Office
Washington, DC 20548

September 13, 2001

The Honorable Van Zeck
Commissioner
Bureau of the Public Debt

Subject: Bureau of the Public Debt: Areas for Improvement in Computer Controls

Dear Mr. Zeck:

In connection with fulfilling our requirement to audit the U.S. government's fiscal year 2000 financial statements,[1] we audited and reported on the Bureau of the Public Debt's (BPD) Schedules of Federal Debt for the fiscal years ended September 30, 2000 and 1999.[2] Our review of the general and application computer controls over key BPD financial systems was performed as a part of these audits. On August 14, 2001, we issued a Limited Official Use letter to you detailing the results of our review. This excerpted version of the letter for public release summarizes (1) the vulnerabilities we identified and recommendations we made and (2) our follow-up on previously reported vulnerabilities.

This letter presents the results of our tests of the effectiveness of general and application controls that support key automated financial systems and our follow-up on the status of BPD's corrective actions to address vulnerabilities identified in our fiscal years 1999 through 1997 audits.[3] These systems, some of which are operated and maintained by the Federal Reserve Banks (FRB), process investments in and redemption of Treasury securities, generate interest payments, account for the resulting federal debt, and provide financial reports to the public and the federal government. We also assessed the general and application controls over key BPD systems that the FRBs maintain and operate and will be issuing a separate letter to the Board of Governors of the Federal Reserve on the results of our testing.

[1] 31 U.S.C. 331 (e) (1994).

[2] *Financial Audit: Bureau of the Public Debt's Fiscal Years 2000 and 1999 Schedules of Federal Debt* (GAO-01-389, March 1, 2001).

[3] *Bureau of the Public Debt: Areas for Improvement in Computer Controls* (GAO/AIMD-00-269, August 9, 2000).

As we reported in connection with our audit of the Schedules of Federal Debt for the fiscal years ended September 30, 2000 and 1999, BPD's internal control over financial reporting and compliance, including computer controls, was effective. In that report, we did not identify any reportable conditions.[4] However, as discussed in this letter, we identified vulnerabilities involving general and application computer controls that we did not consider reportable conditions but, if left uncorrected, increase the risk of inappropriate disclosure or modification of sensitive information or disruption of critical operations. These vulnerabilities warrant BPD management's attention and action. In light of BPD's and the FRBs' significant reliance on interconnected automated systems to support program operations and to replace manual procedures and paper documents, well-designed and properly implemented general and application controls are essential to protecting BPD's computer resources and ensuring continuity of operations. While performing our work, we communicated detailed information regarding our findings to BPD management. This letter provides an overall assessment and summary of BPD's computer control vulnerabilities and recommendations we made.

Results in Brief

Overall, we found that BPD's general and application controls combined with other management and manual reconciliation controls were effective in ensuring BPD's ability to report reliable financial information and data. Although various management and reconciliation controls help BPD detect potential irregularities or improprieties in its financial data or transactions, these types of compensating controls are not preventive controls. Thus, BPD's computer resources or operating environment are exposed to threats such as unintentional errors or omissions or intentional modification, disclosure, or destruction of data and programs by disgruntled employees or intruders. Thus, the vulnerabilities we note increase the risks of inappropriate disclosure and modification of sensitive data and programs, misuse or damage of computer resources, or disruption of critical operations.

Our fiscal year 2000 audit procedures identified certain general control vulnerabilities in BPD's access controls, systems software, and service continuity. We also identified vulnerabilities in the authorization and accuracy controls over a key BPD financial application maintained and operated at the BPD data center. In addition, we identified vulnerabilities in a database conversion that was completed in fiscal year 2000. Our follow-up on the status of BPD's corrective actions to address vulnerabilities identified in our fiscal years 1997 through 1999 audits found that BPD had corrected or mitigated the risks associated with 16 of the 17 general and application control vulnerabilities discussed in our prior years' reports. Additionally, BPD is in the process of addressing the remaining general control vulnerability discussed in our prior years' reports.

[4] Reportable conditions are matters coming to our attention that, in our judgment, should be communicated because they represent significant deficiencies in the design or operation of internal control, which could adversely affect the organization's ability to meet the objectives of reliable financial reporting and compliance with applicable laws and regulations.

BPD informed us that it agreed with our findings and that, in most cases, it had subsequently corrected or was in the process of correcting the vulnerabilities that we identified.

Background

The Department of the Treasury is authorized by Congress to borrow money on the credit of the United States to fund operations of the federal government. Within Treasury, BPD is responsible for prescribing the debt instruments, limiting and restricting the amount and composition of the debt, paying interest to investors, and accounting for the resulting debt. In addition, BPD has been given the responsibility for issuing Treasury securities to trust funds for trust fund receipts not needed for current benefits and expenses.

As of September 30, 2000 and 1999, federal debt managed by BPD totaled about $5,659 billion and $5,641 billion, respectively, for moneys borrowed to fund the government's operations. These balances consisted of approximately (1) $3,439 billion as of September 30, 2000, and $3,668 billion as of September 30, 1999, held by the public, and (2) $2,220 billion as of September 30, 2000, and $1,973 billion as of September 30, 1999, of intragovernmental holdings, such as the Social Security trust funds. Total interest expense on federal debt managed by BPD for fiscal years 2000 and 1999 was about $366 billion and $356 billion, respectively.

BPD relies on a number of interconnected financial systems and electronic data to process and track the money that is borrowed and to account for the securities it issues. In addition, BPD is moving toward Web-based applications to process securities it issues and is relying less on manual procedures and paper documents. FRBs also provide fiscal agent services on behalf of BPD, which primarily consist of issuing, servicing, and redeeming Treasury securities; processing secondary market transactions; and handling the related transfers of funds. The FRBs use a number of financial systems to process debt-related transactions throughout the country. Detailed data initially processed at FRBs are summarized and then forwarded electronically to BPD's data center for matching, verification, and posting to the general ledger.

Objectives, Scope, and Methodology

Our objectives were to evaluate and test the effectiveness of the controls over key financial management systems maintained and operated by BPD and to determine the status of the computer control vulnerabilities identified in our fiscal years 1997 through 1999 audits. We used a risk-based and a rotation approach for testing general and application controls. Under that methodology, every 3 years the data center and each key application is subjected to a full scope review that includes testing in all of the computer control areas defined in our *Federal Information System Controls Audit Manual* (FISCAM).[5]

The scope of our work for fiscal year 2000 included follow-up on vulnerabilities identified in our prior years' reports and FISCAM testing of access controls and system software. For the entitywide security management program area, we benchmarked BPD's *Information Technology Security Manual* to our executive guide on information security management.[6]

To evaluate these general controls, we identified and reviewed BPD's information system general control policies and procedures; observed controls in operation; conducted tests of controls, which included selecting items using a method in which the results are not projectable to the population; and held discussions with officials at the BPD data center to determine whether controls were in place, adequately designed, and operating effectively. Additionally, through our internal network security penetration testing, we attempted to access sensitive data and programs. These attempts were performed with the knowledge and cooperation of appropriate BPD officials.

We also used a rotation approach to evaluate controls over selected key applications. We performed a full scope application controls review of one key financial application to determine whether the application is designed to ensure that

- access privileges establish individual accountability and proper segregation of duties, limit the processing privileges of individuals, and prevent and detect inappropriate or unauthorized activities;
- data are authorized, converted to an automated form, and entered into the application accurately, completely, and promptly;
- data are properly processed by the computer and files are updated correctly;
- erroneous data are captured, reported, investigated, and corrected; and
- files and reports generated by the application represent transactions that actually occur and accurately reflect the results of processing, and reports are controlled and distributed only to authorized users.

The scope of our work on a Web-based financial application covered testing controls over granting access to the program, examining the procedures and guidelines for the creation and use of digital certificates, assessing the appropriateness of the encryption mechanisms, and testing interactive edits and validation of data over the Internet front-end.

The scope of our work on a third key financial application's database conversion covered testing controls over the methodology, test plan standards, test data, test results, and the approval and migration of changes.

[5] *Federal Information System Controls Audit Manual* (GAO/AIMD-12.19.6, January 1999).

[6] *Executive Guide: Information Security Management* (GAO/AIMD-98-68, May 1998).

The scope of our work over four other key financial applications was limited to follow-up on vulnerabilities that we identified in our fiscal years 1997 through 1999 audits.

To evaluate application controls, we identified and reviewed BPD's information system application control policies and procedures; observed controls in operation; conducted tests of controls, which included selecting items using a method in which the results are not projectable to the population; and held discussions with officials at the BPD data center to determine whether controls were in place, adequately designed, and operating effectively.

Because FRBs are integral to the operations of BPD, we assessed the general controls over BPD systems that FRBs maintain and operate. We also evaluated application controls over four key BPD financial applications maintained and operated by FRBs. Further, we followed up on the status of FRBs' corrective actions to address vulnerabilities identified in our fiscal years 1997 through 1999 audits.[7]

To assist in our evaluation and testing of computer controls, we contracted with the independent public accounting firm PricewaterhouseCoopers LLP. We determined the scope of our contractor's audit work, monitored its progress, and reviewed the related work papers to ensure that the resulting findings were adequately supported.

During the course of our work, we communicated our findings to BPD management who informed us that BPD has taken or plans to take corrective action to address the vulnerabilities identified. We plan to follow up on these matters during our audit of the U.S. government's fiscal year 2001 financial statements.

We performed our work at the BPD data center from August 2000 through December 2000. Our work was performed in accordance with U.S. generally accepted government auditing standards. We requested comments on a draft of this letter from the BPD Commissioner. BPD's comments are discussed in the "Agency Comments" section of this letter.

Areas for Improvement in BPD's General Computer Controls

General controls are the structure, policies, and procedures that apply to an entity's overall computer operations. General controls establish the environment in which application systems and controls operate. They include an entitywide security management program, access controls, system software controls, application software development and change controls, segregation of duties, and service continuity controls. An effective general control environment would (1) ensure that an adequate computer security management program is in place, (2) protect data, files, and programs from unauthorized access, modification, disclosure, and destruction, (3) limit and monitor access to programs and files that control computer

[7] *Federal Reserve Banks: Areas for Improvement in Computer Controls* (GAO/AIMD-00-218, July 7, 2000).

hardware and secure applications, (4) prevent unauthorized programs or unauthorized changes to an existing program from being implemented, (5) prevent any one individual from controlling key aspects of computer-related operations, and (6) ensure the recovery of computer processing operations in case of a disaster or other unexpected interruption.

We identified vulnerabilities in the access controls, system software controls, and service continuity controls. These vulnerabilities, if left uncorrected, increase the risk of inappropriate disclosure or modification of sensitive data and programs or disruption of critical operations.

Access Controls

Access controls are designed to limit or detect access to computer programs, data, equipment, and facilities to protect these resources from unauthorized modification, disclosure, loss, or impairment. Such controls include logical and physical security controls.

Logical security control measures involve the use of computer hardware and software to prevent or detect unauthorized access by requiring users to input unique user identifications (ID), passwords, or other identifiers that are linked to predetermined access privileges. Logical security controls restrict the access of legitimate users to the specific systems, programs, and files they need to conduct their work and prevent unauthorized users from gaining access to computer resources.

As we reported in previous audits of BPD's computer controls, there is no periodic user access recertification process being performed between the designated application representatives and the security personnel to help ensure that users are only granted access to applications or systems compatible with their job functions. BPD has historically relied on individual supervisors, as part of their daily employee oversight responsibilities, to monitor access rights assigned to their subordinates. However, BPD did not provide formal guidance to these supervisors to assist them in reviewing access levels of application users. Without a formal recertification process, users who are promoted or reassigned could retain access privileges that are no longer necessary for their current duties, thereby allowing access to system data and functions that could result in a segregation of duties problem and the accidental or intentional modification, destruction, or disclosure of sensitive data. This issue was originally identified as part of our prior years' application testing, and we noted it again as part of this year's application work. Based on this year's results, we have determined that this issue is broader in nature, affecting multiple business applications as well as the mainframe operating system. Accordingly, we reported this issue as a general control weakness in fiscal year 2000.

In assessing the controls over BPD's local area network, we identified several vulnerabilities in network security controls. Specifically, (1) BPD did not consistently perform an independent review of audit logs, (2) BPD had not completed the implementation of a new password expiration policy, (3) some passwords to local accounts on workstations were compromised, but did not allow access to the network domain or to financial applications, (4) no formal polices and procedures existed for reviewing certain user accounts, (5) no formal policies and procedures existed for establishing certain user and group accounts, (6) some system settings were not periodically reviewed and restricted, and (7) BPD personnel were not always using password-protection measures as suggested by BPD's security policy or as required by individual application security plans. These conditions increase the risk that unauthorized activities, such as disclosure of sensitive or proprietary data, may go undetected.

We also noted vulnerabilities in security controls over one financial application server, which resides within BPD's secure network and contains two Web-based applications. The server allows customers such as individual investors of Treasury securities and savings bonds to access certain information from or provide certain information to BPD systems. Specifically, we found (1) the two administrators with access to the server share one account and password, (2) the policy-setting was not consistent with the BPD password standard, (3) several system accounts were unnecessarily given excess access, (4) the IDs and passwords that reside in an isolated environment were not appropriately established, and (5) the monitoring of the environment was limited.

The server architecture, network infrastructure, and security structure make the risk of "external" unauthorized access very low. BPD uses multiple techniques to prevent outside users from having direct access to the network. In addition, we noted other factors that mitigated the risk of several of the vulnerabilities listed above. For example, the administrators could not change any information within the two financial applications.

In addition, we found opportunities to strengthen BPD's password controls over its mainframe access control software. Access control software provides a means of specifying who has access to a system or specific resources and what capabilities authorized users are granted. In several cases, BPD access control password requirements did not comply with suggested industry security standards.

Further, even though BPD has restricted access to its system containing access request and approval information, we identified several documentation deficiencies with the process.

Another important aspect of access controls includes physical security controls, such as locks, guards, badges, alarms, and similar measures (used alone or in combination), that help to safeguard computer facilities and resources from intentional or unintentional loss or impairment by limiting access to the buildings and rooms where they are housed.

During our fiscal year 2000 audit, we assessed the operational effectiveness of BPD's metal detectors and tested the operating procedures for its physical security measures. While we found that the metal detectors were operating effectively, some physical security techniques could be improved upon. Without proper physical safeguards, accidental or intentional destruction of BPD resources could result.

We also observed vulnerabilities in physical security controls over access to the data center during a power outage. We noted that a physical security function that relies on the uninterruptable power supply (UPS) battery did not operate properly. Without a properly operating UPS during an emergency power situation, the risk that individuals can gain unauthorized access to the data center is increased.

System Software

System software coordinates and helps control the input, processing, output, and data storage associated with all of the applications that run on a system. System software includes operating system software, system utilities, program library systems, file maintenance software, security software, data communications systems, and database management systems. Controls over access to and modifications of system software are essential to protect the overall integrity and reliability of information systems.

During our fiscal year 2000 review of system software, we identified vulnerabilities in formal approvals for software acceptance tests that were similar to those noted in our fiscal year 1999 review of BPD's application software development and change control process. Although we are discussing this issue as it relates to software changes, it also applies to application changes. Based on our fiscal year 2000 work, we found that BPD was unable to consistently provide formal written approval on the acceptance test results for system software changes. Specifically, we found the following.

- Four of the 18 system software changes we tested were not approved via the automated approval feature of the problem and change management system. BPD only required verbal approvals, which, according to BPD officials, were obtained during weekly change control meetings prior to introducing changes into the production environment.
- Three of 18 system software changes did not adequately describe the nature of the changes.
- None of the system software change records were used to document the functional areas affected by the changes.
- Five of the 18 system software changes did not contain back-out procedures in the event that the changes were not successful.
- Copies of system software test plans and acceptance test results were not retained in project files for appropriate periods.

Although changes to system and application software are discussed and verbally approved, a formal approval process for software acceptance test results would help ensure and document that system and application software changes migrated to the production environment are properly tested and authorized.

We also found that systems programmers can update critical system software data sets for the operating system's scheduled changes without a documented independent technical review. Systems programmers' activities in making scheduled changes are logged within the operating system and reported in a journal. Each week, staff members review the journal for apparent abnormalities based on their knowledge of the environment and day-to-day system routines. However, the staff does not adequately document its weekly reviews of the access journal. As a result, there is not an adequate management trail for confirming that a particular week's review was actually performed, potentially resulting in inappropriate modifications to critical and/or sensitive data going undetected.

Service Continuity

An organization's ability to accomplish its mission can be significantly affected if it loses the ability to process, retrieve, and protect information that is maintained electronically. For this reason, organizations should have (1) established procedures for protecting information resources and minimizing the risk of unplanned interruptions and (2) plans for recovering critical operations should interruptions occur. A contingency or disaster recovery plan specifies emergency response, backup operations, and postdisaster recovery procedures to ensure the availability of critical resources and facilitate the continuity of operations in an emergency. It addresses how an organization will deal with a range of contingencies, from electrical power failures to catastrophic events, such as earthquakes, floods, and fires. The plan also identifies essential business functions and ranks resources in order of criticality. To be most effective, a contingency plan should be periodically tested in disaster simulation exercises and employees should be trained in and familiar with its use.

In reviewing BPD's service continuity and contingency planning, we found that while progress was being made, corrective actions had not been completed for the vulnerability we identified in our prior years' audits. Although limited recovery tests relating to contingency plan testing have been conducted over the past several years, BPD has never fully tested the complete contingency plan. Without completely testing the full recovery of all critical applications on the system, BPD is at greater risk that it will not be able to recover operations promptly should difficulties occur during an actual emergency.

In fiscal year 2000, BPD had planned to perform a full-system disaster recovery test, including a complete restoration of the operating system and applications residing on the mainframe. BPD successfully conducted the test to restore the operating system of the mainframe. However, tests of mission-critical applications were not performed in fiscal year 2000, primarily due to efforts focused on Year 2000 issues. BPD has prepared a disaster recovery schedule to test all of its mission-critical applications in fiscal year 2001.

BPD's Controls Over Certain Applications Can Be Strengthened

Application controls relate directly to the individual computer programs that are used to perform certain types of work, such as generating interest payments or recording transactions in a general ledger. In an effective general control environment, application controls help to ensure that transactions are valid, properly authorized, and completely and accurately processed and reported.

In addition to testing general controls, we tested application controls for six key financial applications. We identified vulnerabilities in authorization and accuracy controls over one key financial application. We also tested and identified vulnerabilities in one key financial application's database conversion.

Authorization Controls

Authorization controls for specific applications, similar to general access controls, should establish individual accountability and proper segregation of duties, prevent unauthorized transactions from being entered into the application and processed by the computer, limit the processing privileges of individuals, and prevent and detect inappropriate or unauthorized activities.

During our review of the application controls of one key financial application, we identified weaknesses in the authorization documentation used in granting access to the financial application. Of 26 users tested, 4 did not have access request forms on file and 10 users did not have Privacy Act Statement forms on file, acknowledging their responsibility for protecting user and system files from unauthorized access. Of the 22 access forms on file, 10 were not appropriately signed off by program support staff and 1 did not specify to which application the user was granted access or for which functions the user was denied access. Without adequate access request procedures, there is an increased risk that unauthorized access may occur that could result in a segregation of duties problem and the accidental or intentional modification, destruction, or disclosure of sensitive data.

Accuracy Controls

The recording of valid and accurate data into application systems is essential to an effective system that produces reliable results. Accuracy controls include (1) well-designed data entry procedures, (2) data validation and editing to identify erroneous data, (3) reporting, investigating, and correcting erroneous data, and (4) review and reconciliation of output.

During our testing of the edit and validation controls of one key financial application, we noted that edits for two of the application input screens did not always reject data entries containing invalid characters or data values prior to processing. While BPD performs a rigorous data validation process that involves independent re-entering of key data fields and sight verification of the data for accuracy and completeness, the lack of proper automated edits increases the risk of the processing of invalid data for certain of this key financial application's informational screens.

Database Conversion Controls

BPD converted one key financial application database to a new database system in fiscal year 2000. Establishing controls over a database conversion helps ensure that the software modifications are properly authorized, tested, and approved. We reviewed the conversion processes and did not identify any inaccuracies in the converted data. However, we found opportunities to strengthen controls over future database conversions at BPD.

The database conversion was performed without the use of a formal conversion plan tailored specifically to the task. BPD used the Treasury Directive Publication 84-01, *Information System Life Cycle Manual*, as guidance in conducting the conversion. However, the manual provides only generic guidance and is designed to be tailored to reflect the specific characteristics of each individual project. Although, BPD developed guidance to address the acceptance testing aspects of the conversion, the overall conversion documentation was assembled using a piecemeal approach and was never formally documented. As a result, certain critical procedures were either omitted from the overall conversion process, not adequately followed, or not adequately documented. Specifically, we found the following.

- BPD did not have a "fallback" approach documented, there were no postconversion procedures (e.g., updating methodology with lessons learned), and the conversion staff was not provided with proper training.
- BPD did not consistently follow the conversion testing procedures described in its implementation plan. For example, individuals analyzing the test results identified data discrepancies, but did not document the problems or communicate them to management as required by the implementation plan. Consequently, the problems were not resolved prior to the system being moved into production. The exception was corrected only after an end-user identified the problem.
- Documentation supporting the verification of test results was incomplete. Three of 10 sets reviewed lacked proper signatures and dates.

Without a formal, comprehensive conversion plan, critical conversion steps may not be executed, which could lead to inaccurate, incomplete, and inconsistent system data.

FRB Computer Controls Can Be Improved

Because the FRBs are integral to the operations of BPD, we assessed the effectiveness of the general and application controls that support key BPD financial systems maintained and operated by the FRBs. Overall, we found that the FRBs had implemented effective general and application controls. Our fiscal year 2000 audit procedures identified vulnerabilities in general controls that do not have a significant adverse impact on BPD financial systems, but nonetheless warrant FRB management's attention and action. These include vulnerabilities in general controls over (1) access to data, programs, and computing resources, (2) system software, and (3) service continuity. We also found vulnerabilities in authorization controls over four key applications and accuracy controls over one key application. During our follow-up work, we found that the FRBs had corrected the vulnerabilities that were identified in our prior years' reports. We are providing details of these matters in a separate report to the Board of Governors of the Federal Reserve System along with our recommendations for improvement. FRB management has informed us that the FRBs have taken or plan to take corrective actions to address the vulnerabilities we identified. We plan to follow up on these matters during our audit of the U.S. government's fiscal year 2001 financial statements.

Conclusion

Well-designed and properly implemented general and application controls are essential to protect BPD's computer resources and operational environment from the risks of inappropriate disclosure and modification of sensitive information, misuse or damage of computer resources, and disruption of critical operations. BPD needs to take preventive measures to further reduce its exposure to certain threats to its computer resources and operating environment due to unintentional errors or omissions or intentional modification, disclosure, or destruction of data and programs by disgruntled employees, intruders, or hackers. As we noted, BPD has addressed the majority of the vulnerabilities we identified as part of our fiscal years 1997 through 1999 audits and has already taken some actions to resolve the new vulnerabilities we identified during our fiscal year 2000 audit. However, further actions are required to fully address the vulnerabilities discussed in this letter.

Recommendations for Executive Action

In our August 14, 2001, Limited Official Use version of this letter, we recommended that the Commissioner of the Bureau of the Public Debt direct that specific actions be taken to correct each of the individual vulnerabilities that were identified during our testing and summarized in that letter.

We also recommended that the Commissioner of BPD work with the FRBs to implement corrective actions to resolve the computer control vulnerabilities related to BPD systems supported by FRBs, which we identified and communicated to the FRBs during our testing.

Agency Comments

In commenting on a draft of this letter, BPD generally agreed with our findings. The Commissioner of the Bureau of the Public Debt stated that, in most cases, BPD had subsequently corrected or is already taking actions to resolve the issues identified in this letter. In addition to its written comments, the staff of BPD provided technical comments, which have been incorporated as appropriate.

- - - - -

We are sending copies of this letter to the Chairmen and Ranking Minority Members of Senate Committee on Appropriations; Senate Committee on Finance; Senate Committee on Governmental Affairs; Senate Committee on the Budget; Subcommittee on Treasury and General Government, Senate Committee on Appropriations; House Committee on Appropriations; House Committee on Ways and Means; House Committee on Government Reform; House Committee on the Budget; Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, House Committee on Government Reform; and Subcommittee on Treasury, Postal Service, and General Government, House Committee on Appropriations. We are also sending copies of this letter to the Secretary of the Treasury, the Inspector General of the Department of the Treasury, the Director of the Office of Management and Budget, and other agency officials. Copies will also be made available to others upon request. This letter will also be available on GAO's home page at http://www.gao.gov.

If you have any questions regarding this letter, please contact Paula M. Rascona, Assistant Director, at (202) 512-9816. Other key contributors to this assignment were Louise DiBenedetto, Paul Foderaro, and Dawn Simpson.

Sincerely yours,

Gary T. Engel

Gary T. Engel
Director
Financial Management and Assurance

(198033)