Notice:

This document does not currently comply with Section 508 of the Rehabilitation Act of 1973, as amended, 29 U.S.C. § 794d. The OIG is working to become fully compliant with the provisions of Section 508. If you need assistance with accessing the file, please contact the OIG's Office of Audit at (202) 927-5400, or **webmaster@oig.treas.gov** for an accessible edition of the report.

Management Letter for Fiscal Year 2002 Examination of Internal Control Over Financial Reporting at the Bureau of Alcohol, Tobacco and Firearms

OIG-03-045 January 2, 2003

Office of Inspector General

****

The Department of the Treasury

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

JAN 2 2003

OFFICE OF
INSPECTOR GENERAL

MEMORANDUM FOR BRADLEY A. BUCKLES, DIRECTOR
BUREAU OF ALCOHOL, TOBACCO, AND FIREARMS

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

SUBJECT: Management Letter for Fiscal Year 2002
Examination of Internal Control over Financial
Reporting at the Bureau of Alcohol, Tobacco and
Firearms

I am pleased to transmit the management letter in support of the Bureau of Alcohol, Tobacco and Firearms' (ATF) examination of Internal Control over Financial Reporting as of and for the Fiscal Year ended September 30, 2002. KPMG LLP, an independent public accountant (IPA), examined ATF's internal control over financial reporting for its Revenue/Accounts Receivable/Cash Receipts; Procurement/Accounts Payable/Cash Disbursements; Property, Plant and Equipment; and Payroll accounting cycles.

As part of its examination, the IPA issued the accompanying management letter that discusses various issues that were identified during the audit, which were not required to be included in the audit report.

My staff's review of the IPA's working papers determined that the work was performed in accordance with generally accepted government auditing standards. Should you have any questions, please contact me at (202) 927-5430, or a member of your staff may contact Louis C. King, Director, Financial Audits at (202) 927-5774.

Attachment

2001 M Street, NW
Washington, DC 20036

Ronald Collins, Co-COTR
Bureau of Alcohol, Tobacco and Firearms
650 Massachusetts Avenue, NW
Room 4400
Washington, DC 20226

Valarie Smithen-Moore, Co-COTR
Treasury Office of Inspector General
740 15th Street, NW
Suite 600
Washington, D.C. 20220

November 8, 2002

Ladies and Gentlemen:

We have examined the effectiveness of the Bureau of Alcohol, Tobacco and Firearms' (ATF), internal control over financial reporting for its Revenue/Accounts Receivable/Cash Receipts, Procurement/ Accounts Payable/Cash Disbursements, Property, Plant and Equipment, and Payroll accounting cycles (the processes), as of and for the year ended September 30, 2002, based on the *Standards for Internal Control in the Federal Government* (the Standards), issued by the General Accounting Office (GAO) in November 1999 and have issued our report thereon dated November 8, 2002. That report referred to a separate limited official use report that included two reportable conditions related to information technology access-control weaknesses. We have not considered internal control since September 30, 2002.

Our procedures were designed primarily to enable us to form an opinion on the internal controls over financial reporting for ATF's processes regarding the design and effectiveness of internal control in accordance with the Standards and therefore may not bring to light all weaknesses in policies or procedures that may exist. We have attempted, however, to use our knowledge of ATF gained during our work to make comments and suggestions that we hope will be useful to you.

During our engagement, we noted other matters involving internal control and other operational matters that are presented for your consideration in the attachment. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operating efficiencies.

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 audit committee, management, and others within the organization and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP

KPMG LLP. KPMG LLP, a U.S. limited liability partnership, is a member of KPMG International, a Swiss association.

Bureau of Alcohol, Tobacco and Firearms
Comments and Recommendations on Internal Controls
September 30, 2002

1. ***ATF is not performing a reconciliation of the General Ledger System (FReD) to the Fixed-Asset Tracking System (Property Plus System) for Seat Management (ESA) equipment.***

Comment:
The reconciliation between FReD and the Property Plus System is not being performed on a timely basis for ESA equipment. ESA equipment is capitalized leased equipment that is monitored and tracked within the Property Plus System. We noted that disposed equipment that was to be replaced by the newly purchased ESA items was not identified and was not removed from FReD in a timely manner.

Timely reconciliation of detail subsidiary ledgers to the general ledger control accounts is an important control in maintaining accountability for asset management, including the timely recording and disposing of ESA equipment.

By not preparing timely reconciliations between FReD and the Property Plus System for ESA equipment, the risk increases for potential misstatements in the financial statements to occur.

Recommendation:
We recommend that ATF management improve the control activities over asset management by establishing and implementing procedures to adjust FReD on a timely basis for ESA items that have been disposed of through replacement of newly purchased ESA items.

2. ***ATF's current policies allow for certain members of management to sign and approve their own travel vouchers and then submit those travel vouchers to be reimbursed.***

Comment:
Current policies allow for certain members of management to sign and approve their own travel vouchers. We noted one instance in which such a policy may have been the reason for the reimbursement of an expense that did not agree to its supporting documentation.

Maintaining the appropriate segregation of duties by having the review and authorization of the expense reimbursement performed by someone other than the personnel incurring the expense is an important control in maintaining a positive control environment and will decrease the risk of a potential error or fraud.

The current policy could result in ATF's approval and reimbursement of travel expenses that are not appropriate or accurate.

Recommendation:
We recommend that ATF management improve the control activities over the travel expenditures reimbursement process by revising the current travel-expense approval policy to preclude instances where employees that generate expenses are permitted to approve their own expense reimbursements.

We do note that ATF has developed a new delegation that requires independent approval of vouchers for senior-level ATF managers. The new delegation order is targeted for publication in November 2002.

(Continued)

3. ***An ATF employee, possessing an ATF purchase/credit card, did not submit a receipt for a purchase made using the card.***

Comment:
We noted one instance where an ATF employee did not submit a receipt for a purchase made using a credit card. This is a violation of current ATF policy.

Current ATF policy requires purchase card holders to attach their receipts to their purchase card statements. These statements are then to be signed by the cardholder and the approving official and filed in division offices. Reviewing all supporting documentation is an important control in maintaining a positive control environment and will decrease the risk of a potential error or fraud.

Recommendation:
We recommend that ATF management improve the control activities and the control environment over the credit card process by enforcing the guidelines that require the reviewer to obtain and approve the supporting documentation relating to the credit card purchase.

4. ***ATF does not receive or review the SAS 70 reports of service organizations, in order to evaluate the internal controls that ATF relies upon in developing certain financial statement line items.***

Comment:
ATF does not have a current policy or procedure to receive and review the SAS 70 reports for those service organizations that ATF relies on for the processing of transactions relating to the nonentity revenue and human resource processes. The service organizations provide both lockbox services to ATF through a governmentwide agreement and certain payroll services through the United States Department of Agriculture's National Finance Center.

A SAS 70 report includes controls that were tested by an independent accounting firm, the control objectives and the tests applied, and the results of those tests. The results of procedures included in the SAS 70 report would also include user considerations in sufficient detail to permit ATF to take appropriate action to ensure the entire control system is functioning effectively.

A policy to obtain and review the SAS 70 reports will allow ATF to identify and to be aware of control weaknesses of service-providing organizations and to develop expectations of the impact that the weaknesses may have on the financial statements.

When ATF does not review the SAS 70 reports, management may be unaware of control weaknesses that are present in processes that are physically and operationally separate from those maintained at ATF. Additionally, management would not know to establish mitigating controls or to take corrective action on a timely basis.

Recommendation:
We recommend that ATF management improve the control activities over the nonentity revenue and human resource process by developing a policy to obtain the SAS 70 reports from the service

(Continued)

organizations and by establishing and implementing procedures to review the results of those SAS 70 reports and to take corrective action toward any findings.

5. ***The State Occupancy Tax (SOT/FST), Federal Excise Tax (FET), Payroll Processing System (STATS), Property Plus (PPLUS), and Procurement Desktop (PD) systems have expired certification and accreditations.***

Comment:
These five critical financial systems were issued an interim approval to operate on June 11, 2001. The interim approval was for one year and at the time of our review had expired and not been reaccredited. The Information Systems Security Officer was unaware of whether the deficiencies noted in the interim approval had been corrected. The systems are currently operational.

OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," states: "A major application should be authorized by the management official responsible for the function supported by the application at least every three years, but more often where the risk and magnitude of harm is high."

Without a current approval to operate, ATF's critical financial systems increase the risk of operating at a level that is not in compliance with Department of Treasury and ATF Information Technology Policies.

Recommendation:
We recommend ATF management ensure Certification and Accreditation policies and procedures are being followed. Interim accreditation and deficiencies noted need to be corrected prior to the expiration of the accreditation. If deficiencies are not addressed within the allotted timeframe, ATF should place the critical financial systems on a schedule to resubmit their certification packages until all deficiencies have been identified.

6. ***Procurement Desktop (PD), State Occupancy Tax (SOT/FST), Federal Excise Tax (FET), and Payroll Processing System (STATS) did not have all corresponding approving signatures on the access request and deletion forms, as stipulated in ATF 7200.1.***

Comment:
We noted numerous instances where the Information Systems Access form was not being used in accordance with its instructions. For example, the form is not being used to delete users from the PD, SOT/FST, and FET systems; STATS users are being added to the systems without all the required signatures on the access form; and all forms were not maintained on file.

Organizations should have a process for (1) requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions.

Without such a process, the risk of excessive user system access is increased and a complete audit trail of changes to the access-control environment is not available. Without a complete audit trail, the ability to review changes to system access, to track user access, and to ensure proper authorization of user access is reduced.

(Continued)

Recommendation:
We recommend ATF management ensure that Information System Access forms are kept on file for new and deleted users, as well as changes to user access when job functions change. In addition, all signatures should be verified before adding users to the SOT/FST, FET, STATS, and PD systems. A formal annual recertification of users should be done to ensure that users have the least privileged access possible, while still being able to perform their job functions.

Review of documentation on file should examine the level of access each individual has, its conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up to date, whether required training has been completed, and so forth. These reviews can be conducted on at least two levels: (1) on an application-by-application basis or (2) on a systemwide basis.

7. The reconciliation between the HEAT database and the hard copy files was not always complete.

Comment:
Based on our review of the Request for Change forms (RFCs) for the SOT/FST, FET, STATS, and PD systems, the reconciliation between the HEAT database and the hard copy files was not always complete.

In addition, on the RFCs, we noted two out of 29 request for change forms that did not have system owner or change control board chairperson approval signatures.

ATF System Development Life Cycle Handbook, ATF H 7200.2, states: "Functions of configuration management include: control, which is the evaluation, coordination, approval, and implementation of all approved changes to the contents of an established configuration baseline."

ATF Enterprise Architecture Configuration Management Handbook, ATF H 7200.1 states: "For CCB level decisions, all CCB members must initial and date the RFC indicating their approval or disapproval."

Such incomplete reconciliation procedures could lead to changes being made to the production-processing environment without proper review, testing, or approval. This could result in increased production processing problems, inadvertent altering of secure configurations, and potentially malicious code or executables being installed in the production environment.

Recommendation:
We recommend ATF management ensure that all signatures from the system owner, change control board (CCB), and CCB chairperson are included on the RFCs before any changes are made. If the CCB chairperson or an appropriate alternate cannot attend a CCB meeting, the meeting should be postponed until a representative with approving authority can attend.

ATF management should also ensure that all signatures from the system owner, CCB, and CCB chairperson are included on the RFCs before any changes are made.

(Continued)

8. *Simplified Time and Attendance Tracking System (STATS) contingency-planning deficiencies*

Comment:
We noted that STATS contingency-planning documents were not being properly reviewed, updated, and authorized by the appropriate authority, as evidenced by the following:

- The STATS contingency plan has not been updated to address procedures for backup files being rotated off-site.
- Management did not sign the STATS contingency plan.
- The backup processing facility was not identified in the STATS contingency plan.

A complete, updated, and currently approved contingency plan is necessary to ensure effective STATS recovery procedures are followed in the event of a disaster.

National Institute of Standards and Technology, Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems,* states: "It is essential that the contingency plan be reviewed and updated regularly, as part of the organization's change-management process, to ensure new information is documented and contingency measures are revised if required." This review for accuracy and completeness should occur at least annually.

The ATF Emergency Management Program, ATF B 1730.2, also states that: "COOP plans must be maintained at a high level of readiness, capable of implementation both with and without warning."

Recommendation:
We recommend ATF management ensure that procedures for rotating backup tapes off-site be included in the contingency plan. A backup facility should also be identified within the contingency plan. The STATS contingency plan needs to be finalized, signed, and approved by the appropriate authority.

9. *Simplified Time and Attendance Tracking System password weaknesses*

Comment:
Based on our review of STATS access controls, we believe password parameter settings include the following weaknesses:

- ATF's STATS application is operating on U.S. Customs' mainframe. U.S. Customs' mainframe security parameters are not in accordance with security guidelines of NIST 800-47.
- ATF and U.S. Customs are in compliance with the Department of Treasury password standard; however, the Department of Treasury password standard is not in compliance with NIST 800-47.

National Institute of Standards and Technology, Special Publication 800-47 *Security Guide for Interconnecting Information Technology Systems,* 4.2.1 Substep 1, "Implement or Configure Security Controls" states: "If passwords are used, they should be at least eight character long, have a mixture of alphabetic and numeric characters, and be changed at predetermined intervals."

Poor password security parameters subject critical ATF information to the potential for unauthorized access and may prevent ATF from detecting unauthorized access on the system.

(Continued)

Recommendation:
We recommend the Department of Treasury increase the password minimum requirement from six characters to eight special characters. Additionally, we suggest ATF encourage U.S. Customs to make the necessary changes to conform to the security guidelines of NIST 800-47 publication for securing the STATS application.

10. An off-site backup tape storage facility has not been designated for Special Occupancy Tax/Floor Stocks Tax (SOT/FST) and Federal Excise Tax (FET).

Comment:
An off-site backup tape storage facility has not been designated for SOT/FST and FET. Currently the backup tapes reside at the home of a National Revenue Center Information System Division employee.

National Institute of Standards and Technology, Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems,* states: "It is essential that the contingency plan be reviewed and updated regularly, as part of the organization's change-management process, to ensure new information is documented and contingency measures are revised if required." This review for accuracy and completeness should occur at least annually.

Without documented procedures to clearly define the process for housing backup tapes and the designation of a backup tape facility, for SOT/FST and FET, ATF increases the risk of not being able to restore critical information if need arose.

Recommendation:
We recommend ATF management ensure that a backup facility be identified within the contingency plan. Additionally, backup tapes should not be maintained at an employee's home. If necessary, an alternative storage location, such as a bank safekeeping department, should be used until a permanent backup facility is identified.

11. Service Continuity Weaknesses

Comment:
The ATF Continuity of Operations Plan is a working draft and has not been formally approved by the appropriate authority. The disaster recovery system document, dated May 2002, does not have a documented approval signature or distribution list attached.

The ATF Emergency Management Program, ATF B 1730.2, states that: "COOP plans must be maintained at a high level of readiness, capable of implementation both with and without warning."

Because these documents have not been thoroughly reviewed and approved, in the event of a disaster procedures may not be able to be followed properly. While changes are being made to the disaster recovery system document, current interim procedures are not being maintained.

(Continued)

Recommendation:
We recommend ATF management ensure that ATF Continuity of Operations Plan is finalized and formally approved by the appropriate authority and then distributed to responsible parties.

12. ATF Segregation of Duties Weakness

Comment:
Although ATF's IT operations demonstrate an awareness of the importance of segregation of duties between the Finance Management Division and the Information Systems Division through job descriptions and organization charts, we noted that a formally documented segregation of duties policy to address compatible and incompatible duties for the functions shown below is not in place.

Systems Design is incompatible with *Computer Operations*
Computer Operations is incompatible with *Data Administration*
Security Administration is incompatible with *Systems Design*

A lack of segregation of duties between the incompatible duties noted above elevates the potential for unauthorized changes to data to be made and concealed. Employees who otherwise are aware of the importance of segregation of duties may see the lack of a specific formal policy as justification for performing incompatible duties when they believe it is more efficient to do so.

Recommendation:
We recommend ATF management consider enhancing the ATF Management Control Improvement Program by implementing a specific segregation of duties policy to specifically address incompatible duties.