Auditors' Reports

KPMG

2001 M Street, NW
Washington, DC 20036

Independent Auditors' Report on Financial Statements

Inspector General
U.S. Department of Justice

Director
Bureau of Alcohol, Tobacco, Firearms and Explosives

We have audited the accompanying consolidated balance sheet of the U.S. Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), as of September 30, 2003, and the related consolidated statements of net cost, changes in net position, financing, and custodial activities, and the combined statement of budgetary resources for the period from January 24, 2003 (Inception) to September 30, 2003. These financial statements are the responsibility of the ATF's management. Our responsibility is to express an opinion on these consolidated and combined financial statements based on our audit.

We conducted our audit in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards,* issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 01-02, *Audit Requirements for Federal Financial Statements.* Those standards and OMB Bulletin No. 01-02 require that we plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement. An audit includes examining, on a test basis, evidence supporting the amounts and disclosures in the financial statements. An audit also includes assessing the accounting principles used and significant estimates made by management, as well as evaluating the overall financial statement presentation. We believe that our audit provides a reasonable basis for our opinion.

In our opinion, the consolidated and combined financial statements referred to above present fairly, in all material respects, the financial position of the ATF as of September 30, 2003, and its net costs, changes in net position, budgetary resources, reconciliation of net costs to budgetary obligations, and custodial activities for the period from January 24, 2003 (Inception) to September 30, 2003, in conformity with accounting principles generally accepted in the United States of America.

The information in the Management's Discussion and Analysis and Required Supplementary Information sections is not a required part of the financial statements but is supplementary information required by accounting principles generally accepted in the United States of America or OMB Bulletin No. 01-09, *Form and Content of Agency Financial Statements.* We

have applied certain limited procedures, which consisted principally of inquiries of management regarding the methods of measurement and presentation of this information. However, we did not audit this information and, accordingly, we express no opinion on it.

In accordance with *Government Auditing Standards*, we have also issued reports dated November 26, 2003, on our consideration of the ATF's internal control over financial reporting and its compliance with certain provisions of laws and regulations. Those reports are an integral part of an audit performed in accordance with *Government Auditing Standards*, and should be read in conjunction with this report in considering the results of our audits.

KPMG LLP

November 26, 2003

KPMG

2001 M Street, NW
Washington, DC 20036

Independent Auditors' Report on Internal Control

Inspector General
U.S. Department of Justice

Director
Bureau of Alcohol, Tobacco, Firearms and Explosives

We have audited the consolidated and combined financial statements of the U.S. Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) as of September 30, 2003, and for the period from January 24, 2003 (Inception) to September 30, 2003, and have issued our report thereon dated November 26, 2003.

We conducted our audit in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards,* issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 01-02, *Audit Requirements for Federal Financial Statements.*

In planning and performing our audit, we considered the ATF's internal control over financial reporting by obtaining an understanding of the ATF's internal control, determining whether internal controls had been placed in operation, assessing control risk, and performing tests of controls in order to determine our auditing procedures for the purpose of expressing our opinion on the consolidated and combined financial statements. We limited our internal control testing to those controls necessary to achieve the objectives described in OMB Bulletin No. 01-02 and *Government Auditing Standards.* We did not test all internal controls relevant to operating objectives as broadly defined by the Federal Managers' Financial Integrity Act of 1982. The objective of our audit was not to provide assurance on the ATF's internal control over financial reporting. Consequently, we do not provide an opinion thereon.

Our consideration of internal control over financial reporting would not necessarily disclose all matters in the internal control over financial reporting that might be reportable conditions. Under standards issued 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 the internal control over financial reporting that, in our judgment, could adversely affect the ATF's ability to record, process, summarize, and report financial data consistent with the assertions by management in the financial statements.

Material weaknesses are reportable conditions in which the design or operation of one or more of the internal control components does not reduce to a relatively low level the risk that misstatements, in amounts that would be material in relation to the financial statements being

audited, may occur and not be detected within a timely period by employees in the normal course of performing their assigned functions. Because of inherent limitations in any internal control, misstatements due to error or fraud may occur and not be detected.

We noted certain matters, described in Exhibit I, involving the internal control over financial reporting and its operation that we consider to be reportable conditions. However, none of the reportable conditions are considered to be material weaknesses. Exhibit II presents the status of prior year reportable conditions.

As required by OMB Bulletin No. 01-02, with respect to internal control related to performance measures determined by management to be key and reported in the Management's Discussion and Analysis section of the Accountability Report, we obtained an understanding of the design of significant internal controls relating to the existence and completeness assertions. Our procedures were not designed to provide assurance on internal control over reported performance measures, and, accordingly, we do not provide an opinion thereon.

We also noted other matters involving internal control and its operation that we have reported to the management of the ATF in a separate letter dated November 26, 2003.

This report is intended solely for the information and use of the ATF's management, the Department of Justice Office of the Inspector General, OMB, and Congress and is not intended to be and should not be used by anyone other than these specified parties.

KPMG LLP

November 26, 2003

Exhibit I

Reportable Conditions

The ATF must implement effective IT general access and system software controls to address vulnerabilities.

We reviewed the design and operating effectiveness of ATF's general controls for the information technology systems. Our procedures included interviewing ATF management and staff, reviewing supporting documentation, and performing specific tests. We also performed external and internal penetration tests and conducted a vulnerability assessment that included assessing the control structures in place to ensure the information systems data remains reliable, accurate, and complete. Our review focused on various portions of the IT environment as it relates to the processing of financial information.

Using guidance outlined in the General Accounting Office's *Federal Information System Controls Audit Manual* (FISCAM), dated January 1999, we reviewed the following four areas: entity-wide security program planning and management, access control, system software, and segregation of duties. We also relied upon guidance in technical publications issued by the National Institute of Standards and Technology (NIST) and as established in OMB Circular A-130, *Management of Federal Information Resources*. Overall, we ensured adequate coverage of general and application controls through follow-up performed on issues resulting from prior year financial reviews.

The ATF has shown improvement in the areas of entity-wide security, access control, service continuity, change controls, segregation of duties, and applications controls. However, we found certain conditions still exist from prior year audits that indicate the ATF needs to continue to improve its general controls. For example, the information systems lack documented and approved policies and procedures that specify secure operating systems configurations for communication services, access controls, and implementing system modifications. Further, there are information systems weaknesses related to database access and security controls.

Specifically, during our testing, we noted the following:

- Controls over financial network operating systems can be more effectively managed—Various operating systems on the financial network that provide user connectivity to the ATF systems have not been configured to reduce the risk of circumventing security controls. It is critical to develop policies and procedures for configuring network devices, in order to minimize the risk of unnecessary functionality remaining enabled within the network that could result in the security controls being circumvented.
- Access controls over various financial and operational databases need to be strengthened—Database authentication and authorization controls have not been effectively implemented to prevent unauthorized access. For example, weak database system accounts and passwords were identified, as well as excessive access and privileges. These weaknesses cause a lack of segregation of duties and user accountability, which could result in unauthorized database changes and users not being accountable for actions executed on the system.

The Office of Management and Budget, Circular Number A-130, *Security of Federal Automated Information Resources*, requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. In every general support system, a number of technical, operational, and management controls are used to prevent and detect harm. Such controls include individual accountability, "least privilege," and separation of duties.

These general access controls and system software vulnerabilities could compromise ATF's design and operating effectiveness over the information technology systems, as well as the secu-

rity and reliability of the financial data. ATF needs to strengthen controls and processes to prevent these vulnerabilities from recurring.

Recommendation No. 1

We recommend that the Director, ATF review the network services and ports and disable any that are unnecessary. Additionally, ATF should review and update current policies and procedures to provide clear guidelines for approving services that will run on servers attached to the network.

Recommendation No. 2

We recommend that the Director, ATF complete an inventory of all databases within the environment and ensure all the default passwords have been removed, user and developer access is appropriate, and database server passwords are in compliance with ATF password requirements. ATF should also develop policies and procedures to ensure the database server is periodically scanned for weak or default passwords.

Exhibit II

Status of Prior Years' Recommendations

Reported Condition	Recommendations	Status
Information Systems. The ATF needs to strengthen the general controls over its information systems. FY 2002 ATF *Limited Official Use Review of General and Selected Application Controls,* Appendix A, General Controls, dated November 8, 2002.	1. MONITORING ACCESS & USE OF SYSTEMS—Audit the network for the existence of network applications running on the servers and disable them where they are not needed. Furthermore, establish and enforce clear guidelines for approving which services will run on servers attached to the network. 2. PHYSICAL CONTROL—Create a policy that ensures any non-ATF laptop is registered with facilities management. Additionally, ensure security guards monitor incoming laptops and inspect the associated documentation. 3. DATABASE MANAGEMENT-AUTHORIZATION—Implement a phased approach to achieving a more secure database environment. 4. DATABASE MANAGEMENT-AUDITING CONFIGURATIONS—Auditing should be established at the database server level to ensure that no unauthorized users are removing data from the data dictionary or accessing tables for which they should not have privileges. Specifically, an audit plan should be developed to ensure security-related events are recorded. 5. NETWORK DEVICES—Network devices should be configured to enforce Telnet authentication. Also, the Simple Network Management Protocol (SNMP) community name of "public" should be changed to something difficult to deduce or guess. 6. LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL—The Lightweight Directory Access Protocol server should be configured to disallow anonymous connections. Additionally, the SNMP default community name of "public" should be changed to a name that is difficult to deduce or guess.	1. In process 2. Closed 3. In process 4. In process 5. Closed 6. Closed
Information Systems. The ATF needs to strengthen the application controls over its information systems. FY 2002 ATF *Limited Official Use Review of General and Selected Application Controls,* Appendix B, Application Controls, dated November 8, 2002.	1. SEGREGATION OF CRITICAL FINANCIAL APPLICATIONS AND INFORMATION SYSTEMS DUTIES—Ensure the implementation of additional access controls over Property Plus (PPLUS) and Procurement Desktop (PD), including enhancing the segregation of duties between security administrators and data entry personnel. If there is a lack of sufficient resources, a possible solution may be to implement a peer review process by which PPLUS and PD security administrators/alternates periodically monitor/review other security administrators'/alternates' data entry activities. In addition, ATF should consider enhancing the ATF Management Control Improvement Program to specifically address segregation of duties by developing a formal segregation of duties policy, including identification of specific incompatible duties. 2. REVIEW OF ACCESS MONITORING LOGS—Ensure that PPLUS access logs are reviewed on a weekly basis.	1. Closed 2. Closed

As required by *Government Auditing Standards* and OMB Bulletin No. 01-02, *Audit Requirements for Federal Financial Statements,* we have reviewed the status of prior years' findings and recommendations. The following table summarizes these issues and provides our assessment of the progress the ATF has made in correcting these reportable conditions.

2001 M Street, NW
Washington, DC 20036

Independent Auditors' Report on Compliance with Laws and Regulations

Inspector General
U.S. Department of Justice

Director
Bureau of Alcohol, Tobacco, Firearms and Explosives

We have audited the consolidated and combined financial statements of the U.S. Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) as of September 30, 2003, and for the period from January 24, 2003 (Inception) to September 30, 2003, and have issued our report thereon dated November 26, 2003.

We conducted our audit in accordance with auditing standards generally accepted in the United States of America; the standards applicable to financial audits contained in *Government Auditing Standards,* issued by the Comptroller General of the United States; and Office of Management and Budget (OMB) Bulletin No. 01-02, *Audit Requirements for Federal Financial Statements.*

The management of the ATF is responsible for complying with laws and regulations applicable to the ATF. As part of obtaining reasonable assurance about whether the ATF's financial statements are free of material misstatement, we performed tests of the ATF's compliance with certain provisions of laws and regulations, noncompliance with which could have a direct and material effect on the determination of the financial statement amounts, and certain provisions of other laws and regulations specified in OMB Bulletin No. 01-02, including certain requirements referred to in the Federal Financial Management Improvement Act of 1996 (FFMIA). We limited our tests of compliance to the provisions described in the preceding sentence, and we did not test compliance with all laws and regulations applicable to the ATF. However, providing an opinion on compliance with laws and regulations was not an objective of our audit, and, accordingly, we do not express such an opinion.

The results of our tests of compliance with certain provisions of laws and regulations described in the preceding paragraph, exclusive of FFMIA, disclosed one instance of noncompliance that is required to be reported under *Government Auditing Standards* and OMB Bulletin No. 01-02, and is described below.

OMB Circular A-11, *Preparation, Submission, and Execution of the Budget (Revised 07/25/2003),* Appendix B, requires that lease purchases and capital leases must be fully funded at lease inception. Currently ATF is funding these leases annually.

Under FFMIA, we are required to report whether the ATF's financial management systems substantially comply with (1) Federal financial management systems requirements, (2) applicable Federal accounting standards, and (3) the United States Government Standard General Ledger at the transaction level. To meet this requirement, we performed tests of compliance with FFMIA Section 803(a) requirements.

The results of our tests disclosed no instances in which the ATF's financial management systems did not substantially comply with the three requirements discussed in the preceding paragraph.

This report is intended solely for the information and use of the ATF's management, the Department of Justice Office of the Inspector General, OMB, and Congress and is not intended to be and should not be used by anyone other than these specified parties.

KPMG LLP

November 26, 2003