United States Department of the Interior

Office of Inspector General
Washington, D.C. 20240

April 21, 2003

Memorandum

To: Director, Minerals Management Service

From: Roger La Rouche
Assistant Inspector General for Audits

Subject: Management Issues Identified During the Audit of the Mineral Management Service's Fiscal Year 2002 Financial Statements (No. 2003-I-0044)

We contracted with KPMG LLP, an independent certified public accounting firm, to audit the Minerals Management Service's (MMS) financial statements as of September 30, 2002 and for the year then ended. In conjunction with its audit, KPMG noted certain matters involving internal control and other operational matters that should be brought to management's attention. These matters, which are discussed in the attached letter, are in addition to those reported in KPMG's audit report on MMS's financial statements (Report No. 2003-I-0030) and do not constitute reportable conditions as defined by the American Institute of Certified Public Accountants.

The recommendations will be referred to the Assistant Secretary for Policy, Management and Budget for tracking of implementation, therefore your response should be provided directly to that office. If you have any questions regarding KPMG's letter, please contact me at (202) 208-5512.

Section 5(a) of the Inspector General Act (5 U.S.C. App. 3) requires the Office of Inspector General to list this report in its semiannual report to the Congress.

Attachment

cc: Assistant Secretary for Land and Minerals Management
Assistant Secretary for Policy, Management and Budget
Chief Financial Officer, Minerals Management Service
Director, Office of Financial Management
Comptroller, Minerals Management Service
Chief, Financial Management Branch, Minerals Management Service
Audit Liaison Officer, Land and Minerals Management
Audit Liaison Officer, Minerals Management Service
Focus Leader for Management Control and Audit Followup,
Office of Financial Management

2001 M Street, N.W.
Washington, D.C. 20036

March 31, 2003

Office of Inspector General and
Director of Minerals Management Service
Department of the Interior:

We have audited the consolidated balance sheets of the Minerals Management Service (MMS) as of September 30, 2002 and 2001, and the related statements of custodial activity for the years then ended, and the related consolidated statement of net cost, consolidated statement of changes in net position, combined statement of budgetary resources, and consolidated statement of financing for the year ended September 30, 2002, and have issued our report thereon dated December 2, 2002. In planning and performing our audit of the above financial statements of MMS, we considered internal control in order to determine our auditing procedures for the purpose of expressing our opinion on the financial statements. An audit does not include examining the effectiveness of internal control and does not provide assurance on internal control. We have not considered internal control since the date of our report.

During our audit we noted certain matters involving internal control and other operational matters that are presented for your consideration. 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 and are summarized as follows:

1. **Improve Network Security**

   Condition

   MMS has implemented improved configuration management procedures and controls to protect information resources through firewall filtering of inbound and outbound protocols and Intrusion Detection Systems sensors, which are tuned for current attack profiles. However, while no unauthorized access was obtained during our external penetration test work, certain vulnerabilities existed on selected networked systems and devices. We found external and internal vulnerabilities involving unnecessary access to network services and default installations of system software. Specifically, the following medium-risk network security control weaknesses were identified:

   - Numerous open ports on the firewall for the New Orleans site and on a contractor-managed router outside the MMS firewall pose an unnecessary security risk to MMS's network, since many of these ports are used by commonly probed and attacked services; and
     Unnecessary and improperly configured services were observed on one web server that could allow unauthorized access for changing and/or obtaining information.

The detailed scan results (raw data) containing vulnerable IP addresses were provided to MMS network management.

Criteria

OMB Circular A-130, "Security of Federal Automated Information Resources," states that agencies are required to establish controls to assure adequate security of 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. Individual accountability consists of holding someone responsible for his/her actions. In a general support system, accountability is normally accomplished by identifying and authenticating users of the system and subsequently tracing actions on the system to the user who initiated them. Least privilege is the practice of restricting a user's access (to data files, to processing capability, or to peripherals) or type of access (read, write, execute, delete) to the minimum necessary to perform his job. Appendix III also directs that Federal agencies to follow the guidance of the National Institute of Standards and Technology (NIST).

Cause

Vulnerability of the systems existed as a result of these contributing factors:

- Inadequate firewall policy for the New Orleans site and contractor-managed router; and
- Inability to apply software patches or disable unnecessary web server extensions in a reasonable amount of time.

Effect

The vulnerabilities increase the risk that critical MMS systems, including those containing business information, could be compromised or disabled by malicious or unauthorized use. Excessive network services available through open ports and unpatched system software provide unauthorized users with the potential for gaining access to the MMS internal network and then proceeding to compromise system and network availability, confidentiality and integrity.

Recommendation

We recommend MMS management take the necessary steps to improve network security, which should include, at a minimum:

a). Immediately closing the open ports which present a critical risk;
b). Conducting a detailed review of the scan results which have been provided by KPMG in order to determine if other open ports present vulnerabilities for the MMS Network;
c). Disabling or replacing vulnerable network services, including web server extensions. Use protocol filtering to permit only authorized machines to use network services (at router, switch, or firewall); and
d). Applying the latest vendor security patches for the Internet Information Server (IIS) web server.

2. Improve Controls Related to Prompt Pay

Condition

Not all invoices for payment were paid within timelines prescribed within the Prompt Payment Act. During our testing we noted significant improvements in the payment process and ensuring the timely submission of payment. However, we noted that for 2 of the 247 sample items tested, expenses were not promptly paid within the time period allotted, as specified by the Prompt Payment Act (5CFR Part 1315) and the Federal Acquisition Regulation, Paragraph 52.232-25, and interest payments to the vendor were not made for these items. The total value of these items was $118,796 and the associated unpaid interest was approximately $670. When you project this error to the remaining population, our estimate of the unpaid interest in the remaining population is approximately $14,306.

Criteria

The Prompt Payment Act (5 CFR Part 1315) requires Federal agencies to pay expenses on a timely basis, within 30 days of the latter of receipt of an invoice or delivery of goods/services. In the event expenses are not paid within the allotted time period, the Prompt Payment Act further states that interest penalties are to be assessed against the expense and due to vendors along with payment.

Cause

The approving official did not promptly send approved invoices for payment to the Financial Management Branch. Timely receipt of the approved invoice by FMB is imperative for complying with the regulations set forth in the Prompt Payment Act and the Federal Acquisition Regulation. The Financial Management Branch did not pay interest on the two delinquent payments noted in the condition due to management oversight.

Effect

Failure to make timely payments could, if determined to have a direct and material impact, result in a non-compliance with laws and regulations.

Recommendation

We recommend that management ensure that the Procurement Division promptly submits approved vendor invoices to the Financial Management Branch to ensure payments are made in accordance with the Prompt Payment Act and Federal Acquisition Regulation. In the event invoices are not submitted in a timely fashion, the Financial Management Branch should calculate the interest expense incurred for non-compliance with the Prompt Pay Act and submit interest payments to vendors accordingly and promptly.

Our audit procedures are designed primarily to enable us to form an opinion on the financial statements, and therefore may not bring to light all weaknesses in policies or procedures that may exist. We aim, however, to use our knowledge of MMS gained during our audit to make comments and suggestions that we hope will be useful to you.

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 Department of the Interior's management, Department of the Interior's Office of the Inspector General, Office of Management and Budget and the U.S. Congress, and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP