C-IN-OSM-0095-2002-A

United States Department of the Interior

Office of Inspector General
Washington, D.C. 20240

March 17, 2003

Memorandum

To: Director, Office of Surface Mining Reclamation and Enforcement

From: Roger La Rouche Roger LaRoche
Assistant Inspector General for Audits

Subject: Management Issues Identified During the Audit of the Office of Surface Mining Reclamation and Enforcement's Fiscal Year 2002 Financial Statements (No. 2003-I-0035)

We contracted with KPMG LLP, an independent certified public accounting firm, to audit the Office of Surface Mining Reclamation and Enforcement's (OSM) 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 OSM's financial statements (Report No. 2003-I-0022) 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
Chief Financial Officer, Office of Surface Mining Reclamation and Enforcement
Director, Office of Financial Management
Audit Liaison Officer, Land and Minerals Management
Audit Liaison Officer, Office of Surface Mining Reclamation and Enforcement
Focus Leader for Management Control and Audit Followup,
Office of Financial Management

ATTACHMENT

KPMG

Suite 2700
707 Seventeenth Street
Denver, CO 80202

November 15, 2002

The Director of the Office of Surface Mining Reclamation and Enforcement
and the Inspector General of the Department of the Interior:

We have audited the financial statements of the Office of Surface Mining Reclamation and Enforcement (OSM) for the year ended September 30, 2002, and have issued our report thereon dated November 15, 2002. In planning and performing our audit of the financial statements, 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. The maintenance of adequate internal control designed to fulfill control objectives is the responsibility of management. Because of inherent limitations in internal control, errors or fraud may nevertheless occur and not be detected. Also, controls found to be functioning at a point in time may later be found deficient because of the performance of those responsible for applying them, and there can be no assurance that controls currently in existence will prove to be adequate in the future as changes take place in the organization. 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 appropriate members of management, are intended to improve internal control or result in other operating efficiencies and are summarized below. In addition to our 2002 comments and recommendations, we have reported the status of prior year management letter comments. Their current status is addressed in the progress on prior year management letter recommendations section of this letter.

Network Security

Our audit revealed areas relative to the OSM's network security management that require improvement in order to enhance security effectiveness from both external and internal perspectives. Network security control weaknesses were identified as indicated below.

Externally:

a) Network Software Implementation – The OSM's Fee Billing and Collection System (FEEBACS) back-end database financial software is placed on a host that also houses a publicly accessible application known as AVS. The FEEBACS back-end application is not intended to be publicly accessible and, by design, the FEEBACS front-end application is accessible by a web page. The AVS system is publicly accessible via TELNET protocol without TCP wrappers and SSH; screen shots indicate this is the case externally from across the Internet. Because the host is publicly accessible, its IP address can be found from publicly available information. The TELNET session without TCP wrappers and SSH is "in the clear" and is thus vulnerable to successful "sniffing" of login ID and password credentials from anywhere on the Internet.

b) Although AVS is a “read only” application for the majority of users, there are users with “write” access. As such, the potential exists for an unauthorized user or attacker to obtain legitimate access credentials that convey “write” privileges to an area on the shared host. Those write privileges may be used in combination with known Unix exploits and/or malicious scripts to escalate a compromised account to higher levels of access. This may, in turn, allow the attacker to exit the application and establish a session with the operating system of the shared host, which in turn cascades the risk of compromise to the FEEBACS back-end database files.

c) In addition, an exploitable vulnerability was found during an external scan against a web server host. Specifically, we noted predictable TCP Packet Sequence Numbers vulnerability, which reveals the software implementation of the TCP/IP stack on the host and uses a faulty random number generator and should be patched with an updated version. If successfully exploited, this vulnerability can escalate the attacker to a logical position of being able to acquire unauthorized access to the operating system either directly or by “spoofing.”

Internally:

a) Certain hosts’ operating systems installed with common security vulnerabilities.

b) Null session connections allowing enumeration of users and shares.

c) Weak password files (Denver downtown and Washington DC locations), which allowed access to the password file for the host.

d) Three noncurrent accounts on the FEEBACS web server.

The weaknesses identified can permit an attacker to “sniff” TELNET logins onto the host platform, thus obtaining a means of accessing the AVS/FEEBACS back-end host with some level of authorized “privilege.” If the FEEBACS database is not properly “locked down” (i.e., host based IDs, auditing turned on, nonshared administrative accounts), the probability exists that an attacker with intermediate skills can compromise the AVS application, escalate the privilege set, and successfully attack/compromise the FEEBACS back-end database.

Although many of the vulnerabilities identified above do not directly impact financial systems, the presence of vulnerabilities on nonfinancial systems, increases the risk of penetration to the network overall.

Recommendation

The OSM should take the following steps to improve its network security posture:

a) Review current network configuration and apply all current patches.

b) Improve frequency of network configuration and monitoring.

In addition, to correct the immediate vulnerabilities identified, the OSM should:

c) Separate the FEEBACS back-end database from the AVS and place the FEEBACS back-end database on a separate processing platform that does not host other "publicly available" applications. An alternative solution may be to require that FEEBACS users, with "write" access, use SecureShell when accessing the application.

d) Place the FEEBACS back-end database host in an internally accessible only zone on the OSM intranet.

e) Implement processes to identify and remove in a timely manner all noncurrent accounts on the FEEBACS web server.

OSM Response

The OSM concurs with the above finding and recommendation and offers the following responses to specific recommendations. Item (a), "Review current network configuration and apply all current patches," and item (b), "Improve frequency of network configuration and monitoring," both apply to the findings identified under the heading of "Internally."

With regard to the specific findings in this category, item (a), "Certain hosts' operating systems installed with common security vulnerabilities" and item (b) "Null session connections allowing enumeration of users and shares," both refer to four conditions observed during the internal penetration testing. The first condition is known as IP Forwarding and was discovered to be active on one of the Division of Financial Management's (DFM) Hewlett-Packard 3000 mini-computers. This was a configuration problem and was resolved on August 20, 2002. The second condition has to do with FTP on the same Hewlett-Packard 3000 mini-computer. KPMG is concerned that the version of FTP on this mini-computer is patched to a level that is greater than or equal to WFTPD 2.4.1rc11. The OSM contacted the vendor (Hewlett-Packard) and received documentation that the version of FTP in use on this server is current, and that all known CERTs for FTP are covered in this version.

The third condition has to do with SNMP on this same Hewlett-Packard Server. Again, the OSM contacted the vendor (Hewlett-Packard) and discovered that the current version of SNMP does not comply with all issued CERT's for SNMP. As of November 7, 2002 an updated version of SNMP for the Hewlett-Packard 3000 that does comply with all issued CERT's became available. This patch will be implemented by the end of December 2002.

The fourth condition observed was KPMG's ability to enumerate user names, shares and policy on some of the Windows based servers used throughout the OSM. Upon further investigation by the DFM Systems staff and staff at Microsoft Corporation, it was discovered that the Windows based servers in use at the DFM were all patched for this vulnerability. In fact, closer examination of the detailed penetration reports revealed that the Windows based servers at the DFM would enumerate the user names but not the shares or the policy. This is the current "state of the art" for this Windows operating system and there is nothing more that the DFM can do at this time. The DFM will continue to monitor the availability of patches to further secure this vulnerability.

OSM Response, Continued

Item (c) from the internal penetration testing, "Weak password files (Denver downtown and Washington DC locations) which allowed access to the password file for the host," has been resolved. The administrators for these platforms were informed of this condition shortly after it was identified and steps have been taken to strengthen these passwords.

Item (d) from the internal penetration testing, “Three noncurrent accounts on the FEEBACS web server,” has been resolved. During their testing, KPMG noticed that three user accounts were active on this web server when the individuals were no longer at the DFM. These user accounts were for the developers of the system. At the time of the audit, sporadic development work was still occurring on this web server. While this in no way supports leaving these user accounts active while the developers were not actively engaged in software development, it does provide a reason for why this situation existed. Since that time the DFM has strengthened its procedure for establishing and maintaining user accounts on the web server in such a way that this situation has been eliminated. This satisfies recommendation (e) “Implement processes to identify and remove in a timely manner all noncurrent accounts on the FEEBACS web server.”

Recommendation (c) states “Separate the FEEBACS Back-end database from the AVS and place the FEEBACS Back-end database on a separate processing platform that does not host other “publicly available” applications. An alternative solution may be to require that FEEBACS users, with “write” access, use SecureShell when accessing the application.” OSM would like to note that all of the FEEBACS users that have “write” access are stationed at DFM. Therefore, there are no users with “write” access that are traversing the Internet to gain access to this application. For this reason, the OSM is somewhat comfortable with the fact that FEEBACS and AVS reside on the same physical platform. The OSM will be investigating a number of options for further improving the security of these systems over the next several months and will be evaluating the cost-effectiveness of each.

With regard to recommendation (d), “Place the FEEBACS Back-end database host in an internally accessible only zone on the OSM intranet,” OSM will be investigating a number of options to further improve the security of this system including putting it on a separate platform within our intranet. This investigation will be conducted along with our analysis of options to satisfy recommendation (c) above.

Application Logical Access

Our audit determined that the OSM’s access controls and security policies for applications need improvement. For instance:

a) Changes to the Advanced Budget/Accounting Control and Information System (ABACIS) database are made using the “MGR” group account, rather than through individual accounts. The “MGR” account is designated for application administration and is not to be used for nonadministrative functions.

b) ABACIS system users that should not have access to the “MGR” account password improperly used the group account.

c) Contrary to the OSM’s policy, some changes made to data in the database were not supported by a System Trouble Report (STR) form, which documents the nature and approval of the change.

d) Individual accounts have been assigned to execute ABACIS administration, however, the group “MGR” account continues to be used.

e) OSM management has not developed a security plan for the Federal Personnel and Payroll System (FPPS) application.

f) Access rights to the Hyperion application were active for an individual who had transferred from the accounting department in August 2001. The individual no longer required access to Hyperion to perform required job functions.

Weak logical access controls increase the risk of unauthorized access to the application, which can result in loss, damage or theft of valuable information and/or resources. At a minimum, users can currently obtain access to sensitive data and systems that are not commensurate with their job requirements. In the event of unauthorized access, timely generation and review of security logs could help ensure that security breaches are detected and the source of the breech identified, allowing management to act on violations.

OSM has detailed policies and procedures governing logical security over the ABACIS application. According to OSM management, the importance of STR documentation, and use of only individual accounts has been emphasized, however, compliance with the policy has not been achieved.

It appears the above problems stem from a combination of factors including the need for additional logical access policies, a lack of application security plans, and a lack of management oversight to ensure compliance with current IT policies.

Recommendation

The OSM should implement the following changes to improve access controls over its financial applications:

a) Limit the use of group administration accounts and passwords for the ABACIS application.

b) Increase management oversight over making changes to the ABACIS database, (e.g., consider performing random audits of database changes to ascertain compliance by OSM personnel).

c) Increase management oversight over the termination of access rights for transferred employees to ensure that access rights are removed in a timely manner.

In addition, relative to FPPS and Hyperion, the OSM should direct and support the development and implementation of security plans for these applications. Given FPPS and Hyperion are owned by the Department of the Interior, the security plans should address only those aspects relevant to the OSM. Further, the OSM's security plans should incorporate guidance supplied by the Department.

OSM Response

The OSM partially agrees with the above findings and recommendation and offers the following response.

With respect to item "a" under the Recommendation, the OSM limited knowledge of the group administrator (MGR) User Id and password to 3 people (the primary administrator and 2 backups). This was done in October of 2001. We feel that this is sufficient as it provides an acceptable level of control over the use of the group administrator (User Id) while allowing the OSM to maintain an acceptable backup presence for the primary administrator. We recognize this as an acceptable level of risk in our risk analysis for the Hewlett-Packard server.

Recommendation "b" calls for the OSM to increase management oversight over changes made to ABACIS data and to consider implementing random audits of database changes to ascertain compliance with procedures. The OSM already performs random audits of database changes. The system owners randomly request listings of database log files and review these log files. Whenever a change to data using NMQUERY is noted in the log files, the system owners request a supporting System Trouble Report (STR) for documenting the change. The OSM will continue this process and continue to refine the procedure in order to eliminate any future occurrences of undocumented data changes.

Item “c”, the Hyperion access condition involves a DFM employee who had been transferred from one team to another within the DFM. This individual is a current DFM employee. While it is true that the employee had a user ID for the Hyperion application, the employee never had credentials for the National Business Center's (NBC) citrix server that houses the Hyperion application. Since fiscal year 2000, Hyperion users must first log into the citrix server and then log into the Hyperion application. Under this scenario, the employee could never have accessed the application without the proper server credentials. The employee’s user ID has since been removed from the application.

With regard to the need for security plans for FPPS and Hyperion, the DFM will obtain sample security plans for these systems from another bureau within the Department of the Interior. We will then modify these plans to our particular use of the departmental systems.

System Software

The OSM’s DFM has not developed policies to help ensure the proper monitoring of, access to, and use of its operating system software.

Controls over access to the operating system software are essential in providing reasonable assurance that system-based security controls are not compromised. If related personnel policies for system access controls are not adequate, there is a risk that untrustworthy and untrained individuals may have unrestricted access to software code, terminated employees may have the opportunity to compromise systems, and unauthorized actions may not be detected.

It appears the OSM has not emphasized the development of polices and procedures governing access to and monitoring of operating system software, as they rely on the expertise of the IT department staff and the limited number of individuals with access to system software.

Recommendation

The OSM’s DFM management should develop and implement formal policies and procedures to monitor the access to and use of its system software and utilities.

OSM Response

Management requires each platform administrator to remain current on required patches and upgrades for their areas of responsibility. This is a monthly requirement of our Quality Assurance Program that is monitored by our IT Site Security Officer. It is important to note that due to the rapid implementation of patches and upgrades by the systems staff, the DFM computer environment has not been successfully hacked since the implementation of our rigorous program of maintaining systems at the manufacturers’ recommended release level. Each upgrade to the system comes with explicit instructions from Hewlett Packard (HP), SUN or Microsoft for their appropriate platforms. A consulting firm performs the SUN upgrades. Hewlett Packard is under contract to supply appropriate upgrades and fixes to the HP operating system, including written procedures for implementation. A DFM system administrator performs the NT server patches and upgrades by following Microsoft written and computerized procedures. During the past year the DFM has enhanced the procedures in its Quality Assurance Log book for identifying and implementing upgrades, patches, and updates to system software.

To address the above condition, the DFM has added three management approval checkpoints to the process in order to improve management oversight. The first is a pre-implementation checkpoint where the system administrator will fully explain the update and the reasons for the update to the Team Leader and Financial and Administrative Systems Team. If a particular update is deemed not necessary, this will be indicated in the Quality Assurance Log as well. Once approved by the Team Leader in the Quality Assurance Log, the system administrator will schedule and apply the update. At the end of the procedure an additional signoff will occur where the system administrator “closes out” the process with the Team Leader. The new procedure is as follows:

Procedure for upgrading server system software:

1. Review the present patches or upgrades to the operating system or software.

2. Read all the documentation associated with the patch or upgrade and determine if it is appropriate for implementation.

   If a patch or upgrade is not considered necessary for implementation, provide a short narrative as to why it is not considered necessary and obtain the concurrence of the Team Leader, Financial and Administrative Systems Team (FAST).

   If a patch or upgrade is considered necessary for implementation, the change must be discussed with the Financial and Administrative Systems Team Leader and must have their signed approval prior to proceeding with the implementation.

3. Once a patch or upgrade has been evaluated and the decision has been made to implement, develop and document an implementation plan/schedule. This might include the scheduling of contract vendors or scheduling of computer/host down time.

4. Document how and when the change was implemented.

5. Once the change has been completely implemented, the change is discussed with the Financial and Administrative Team Leader and an approval is required to closeout the upgrade process.

Progress On Prior Year Management Letter Recommendations

The following is a summary of the implementation status of prior year management letter comments.

Comment	Status
Information Technology Contingency Plan – The OSM’s DFM has not performed sufficient testing of its business continuity plan to ensure its ability to fully restore critical systems and data in the event of a significant business interruption.	**Implemented**. Our fiscal year 2002 audit did not identify instances of a lack of testing of the OSM business continuity plan.

Comment	Status
Information Technology Change Control – The OSM had not properly documented changes made to ABACIS. Further, the OSM's change control methodology does not include policies and procedures governing application software libraries, including labeling and/or maintaining an inventory of programs.	**Implemented**. Our fiscal year 2002 audit did not identify instances of undocumented changes made to ABICAS or a lack of policies and procedures governing application software libraries.
Information Technology Logical Access – The OSM needed to improve certain aspects of logical access for applications owned or used by DFM.	**Partially Implemented**. Our fiscal year 2002 audit found the OSM had made some improvements in controls over logical access; however, our audit still found areas of inadequate controls, as discussed above under application logical access.
Information Systems Software – The OSM had not developed policies to help ensure the proper monitoring of, access to and use of operating system software. Further, OSM had not developed formal policies and procedures for controlling changes to its operating system software.	**Partially Implemented**. Our fiscal year 2002 audit found the OSM had made improvements in developing policies and procedures for controlling changes to its operating system software. However, the OSM's DFM has not developed policies to help ensure the proper monitoring of, access to, and use of its operating system software. This outstanding issue is discussed above under the system software comment.
Investment Policies – The OSM had not consistently followed its internal investment policies. It was recommended the OSM improve its procedures to ensure compliance with its own investment policies.	**Implemented**. Our fiscal year 2002 audit did not identify instances of a lack of adherence to internal investment policies.

Comment	Status
Approval of Grant Obligations – The OSM had not consistently documented its approval for establishing grant obligations. It was recommended the OSM improve its procedures to ensure compliance with its internal grant obligation control guidance listed in its Federal Assistance Manual.	**Implemented**. Our fiscal year 2002 audit did not identify instances of a lack of approval for establishing grant obligations.
De-obligating Funds – The OSM had not implemented effective procedures to ensure all inactive undelivered orders were de-obligated in a timely manner. It was recommended the OSM perform a thorough review of all unliquidated obligations and de-obligate invalid undelivered orders in a timely manner throughout the year. .	**Implemented**. Our fiscal year 2002 audit did not identify any significant inactive undelivered orders that were not de-obligated in a timely manner.
Unauthorized Credit Card Use – The OSM did not have adequate procedures to ensure credit cards were used only by the cardholder identified on the card. It was recommended the OSM improve its credit card review procedures.	**Implemented**. Our fiscal year 2002 audit did not identify instances of unauthorized credit card use.

* * * * * * *

Our audit procedures are designed 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 the OSM gained during our work to make comments and suggestions that we hope will be useful to you.

We will be pleased to discuss with you in more detail any of the matters referred to in this letter.

This letter is intended for the information and use of the OSM and Department of the Interior's management, Department of the Interior's Office of the Inspector General, the U.S. Office of Management and Budget (OMB), 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