U. S. Department of the Interior
Office of Inspector General

Audit Report

IMPROVEMENTS MADE IN GENERAL CONTROLS OVER AUTOMATED INFORMATION SYSTEMS

OFFICE OF SURFACE MINING RECLAMATION AND ENFORCEMENT

Picture courtesy of OSM

Report No. 01-I-415
September 2001

U.S. Department o the Interior **Office of Inspector General**

EXECUTIVE SUMMARY

Improvements Made in General Controls Over Automated Information Systems, Office of Surface Mining Reclamation and Enforcement Report No. 01-I-415 September 2001

BACKGROUND

The Office of Surface Mining Reclamation and Enforcement (OSM) is dependent on automated information systems to support its mission and to provide reliable data for its annual financial statements. The Division of Information Systems Management is responsible for facilitating controls and efficient and effective use of information technologies and information resources to support the OSM mission.

OBJECTIVE

The objective of the audit was to determine whether the actions taken by the OSM satisfactorily implemented the 38 recommendations in our prior audit report titled “General and Application Controls Over Automated Information Systems, Office of Surface Mining Reclamation and Enforcement,” (No. 00-I-138) and whether any new recommendations were warranted.

RESULTS IN BRIEF

We concluded that the OSM had made substantial progress in correcting the weaknesses identified in our prior audit report and in improving general controls over the OSM’s automated information systems. Based on actions taken previously and as a result of our current audit, we considered 37 of the 38 recommendations resolved and implemented.

RECOMMENDATIONS

We made four new recommendations to the OSM that should correct the weaknesses identified in our current report.

AUDITEE COMMENTS AND OFFICE OF INSPECTOR GENERAL COMMENTS

The OSM concurred with the report’s four recommendations and agreed to take the recommended corrective actions.

A-IN-OSM-001-00-M

United States Department of the Interior

Office of Inspector General
National Information Systems Office
134 Union Boulevard, Suite 510
Lakewood, Colorado 80228

September 21, 2001

AUDIT REPORT

Memorandum

To: Director, Office of Surface Mining Reclamation and Enforcement

From: Diann Sandy Diann Sandy
Director, National Information Systems Office

Subject: Improvements in General Controls Over Automated Information Systems, Office of Surface Mining Reclamation and Enforcement (No. 01-I-415)

We reviewed the actions taken by the Office of Surface Mining Reclamation and Enforcement (OSM) to determine whether the OSM satisfactorily implemented the 38 recommendations in our December 1999 audit report titled "General and Application Controls Over Automated Information Systems, Office of Surface Mining Reclamation and Enforcement" (No 00-I-138) to improve general controls over the OSM's automated information systems. We also determined whether any new recommendations were warranted. In addition, we performed this audit to support the Office of Inspector General's opinion on the OSM's financial statements by evaluating the reliability of the general controls over automated systems that support the annual financial statements.

RESULTS OF AUDIT

The OSM Improved General Controls Over Its Automated Systems

We concluded that the OSM had made substantial progress in improving general controls over its automated information systems by implementing 37 of the 38 recommendations contained in our prior audit report. We found that before the start of our current audit, the OSM implemented 29 of the 38 recommendations from our prior audit. Based on our current audit, the OSM implemented an additional 8 recommendations. The one prior audit recommendation awaiting implementation pertains to contingency plans. Our current audit made four new recommendations concerning the completion of corrective actions and the improvement of security management and access controls.

The OSM recently improved controls in the following areas.

Risk Management

In our prior report we recommended that risk assessments be conducted (Recommendation A.2). The OSM prepared risk assessments of its five mission-critical information systems, and senior management approved these assessments.

Reviewing Users' Access to Systems

In our prior report we recommended that the OSM develop and implement procedures to periodically review users' levels of access to systems to ensure that the access levels are current and appropriate (Recommendation E.3). The OSM Division of Financial Management completed its review of access levels of all users of its systems, and the OSM has implemented procedures to ensure that periodic reviews of all users levels of access to all OSM systems would be performed.

Notifying System Administrators of Changes in Users' Employment Status

In our prior report we recommended that the OSM develop and implement procedures to promptly notify system administration personnel of users' employment terminations or reassignments of duties (Recommendation E.4). The OSM developed procedures for promptly notifying system administration personnel of system users' employment terminations or reassignments.

Separation of Duties

In our prior report we recommended that policies and procedures be implemented to ensure separation of duties between reviewing and controlling system logs and administering system access controls (Recommendations K.3 and M.1). In addition, we recommended that application programmers should not be responsible for moving changed software into the production environment and should not have access to update or change production data (Recommendation M.2). The OSM developed policies and procedures for maintaining, controlling, and reviewing system logs and ensured that personnel who were responsible for maintaining the logs did not review or control the logs or administer access to the systems. In addition, the OSM implemented procedures, which it believes alleviates the separation of duty risks, for moving changed software to the production environment. Further, in the OSM's next risk analysis, the OSM will address the risk associated with the separation of duties in moving changed software into production and ensure that OSM management officials accept any residual risk.

Software Development and Change Management Controls

In our prior report we recommended that the OSM's policies and procedures for software development and change management be enforced (Recommendation N.1). The OSM developed policies to ensure that all application software changes are properly authorized, tested, and approved prior to being moved into production and that access to software programs is controlled. In addition, the OSM established an Independent Security Officers Review Team to perform periodic reviews of software development and change management to ensure that OSM policies are followed.

Further Improvement in System Security Management and Access Controls Are Needed

We found that further improvements are needed in the following areas.

Finalize and Test System Contingency Plan

In our prior report we recommended that contingency plans intended for telecommunications links, facilities, and the data center be finalized and tested and that test results be used to update these plans. Additionally, we recommended that assurance should be provided that personnel are trained to implement the plans (Recommendation O.2). The OSM had not finalized the systems contingency plan and had not tested the continuity of operations plan for the OSM headquarters operations. The OSM officials said that the planning for service continuity was ongoing but the plan had not been completed, approved, and finalized. Until the headquarters contingency planning is completed and tested, the OSM remained vulnerable to loss of systems operations caused by a loss of computing capability due to an unexpected event.

Reevaluate Position Sensitivity Classifications

Although the OSM implemented personnel security policies and procedures, we found that position sensitivity classifications were not always based on the duties and risks of the positions. For example, system administrator positions that had full access and control over systems were not designated as critical public trust positions. Without adequate classification of positions warranting critical public trust and the commensurate security clearances, the risk was increased that the OSM systems could be compromised or impaired. The OSM needs to reevaluate its positions for performing information systems duties to determine the inherent security risks and sensitivity of these positions and properly classify the positions of high risk.

New User Access

The OSM policy requires granting access to new users of systems to be documented and approved by system security managers or system owners. We found, however, that access was granted to the Applicant Violator System (AVS), which is a major application, based on verbal requests via telephone communication. Granting access to the AVS by verbal request does not ensure that the request is authentic and that responsible managers or supervisors have authorized the new user access request. Using this type of authorizing procedure subjects the AVS to the risk of unauthorized use and uncontrolled acts. The OSM needs to ensure that new user access to the AVS is granted in accordance with established OSM access control procedures.

Remote Access

The OSM had established remote access connectivity to some of its information systems via dialup to a modem pool; however, all available security practices to control unauthorized dialup access were not implemented. For example, we found that the telephone numbers for the remote-access modem pool were not periodically changed and that a call-back feature to specifically authorized remote-user telephone numbers was not implemented. Additionally, the OSM had not established other available security measures for remote-access users (via modem and the Internet from home computers) such as requiring specific virus protection on the remote computers. The OSM management needs to strengthen remote access controls and safeguards to protect the OSM systems from unauthorized intrusion, virus threats, and cyber attacks.

Recommendations

We recommend that the Director, OSM:

1. Fully implement our prior report Recommendations A.2, C.1, E.3, E.4, K.3, M.1, M.2, N.1, and O.2; or institute other alternative or compensating controls adequate to correct the weaknesses; or if certain weaknesses are an acceptable risk, document the risk acceptance in a formal (management approved) risk assessment.

2. Reevaluate the appropriateness of designated sensitive or high risk positions and the respective duties and obtain the necessary security clearances for personnel filling these sensitive or critical public trust positions.

3. Ensure that the OSM's established policies and procedures are followed when granting new users' access to the Applicant Violator System.

4. Establish remote-access control procedures and remote user-set parameters and strengthen the existing practices by providing added control features and required settings or document the acceptance of risk in a formal (management approved) risk assessment.

OSM Response and OIG Reply

Based on the May 30, 2001 (Appendix 2) and July 3, 2001 (Appendix 3) responses, we consider Recommendation 1 resolved but not implemented and have requested additional information for Recommendations 2, 3, and 4. The OSM agreed with the recommendations, but needs to provide target dates for implementation of actions planned and titles of officials responsible for implementation. The May 30, 2001 response to Recommendation 1 stated that the only remaining corrective actions regarding our prior report's recommendations would be to complete Recommendation O.2 during June and August 2001. Additionally, the OSM provided the latest draft version of the Continuity of Operations Plan (Management Plan, Test Plan, and Schedule) for its headquarters systems operations. As stated in the Results of Audit section, the OSM draft plan still needs to be finalized and tested.

Background

The mission of the OSM is to implement the provisions of the Surface Mining Control and Reclamation Act and to ensure that society and the environment are protected from the adverse effects of surface and subsurface coal mining operations. The OSM activities include issuing mining permits, inspecting mining operations, enforcing mining standards, ensuring the effectiveness of authorized state and tribal regulatory programs, and promoting reclamation of surface mine lands.

The OSM is dependent on automated information systems to support its mission and provide reliable data for its financial statements. The Division of Information Systems Management is responsible for facilitating the systems controls and efficient and effective use of information technologies to support the OSM mission. Various OSM organizations, including the Division of Information Systems Management, the Division of Financial Management, assistant directorates, and regional and field offices share responsibilities over the OSM systems. Nationwide, automated data processing support is provided through local area network-based servers and microcomputer workstations, and the networks are interconnected by the OSM-wide area network.

Scope and Methodology

Our audit was conducted at the OSM's headquarters in Washington, D.C., and its data center in Denver, Colorado. Our audit was performed in accordance with the "Government Auditing Standards," issued by the Comptroller General of the United States. Accordingly, we included such tests of the records and other auditing procedures that were considered necessary under the circumstances. Additionally we used the review methodologies contained in the U.S. General Accounting Office's "Federal Information System Controls Audit Manual." As part of our review we evaluated only the internal controls related to the general control environment over the OSM's automated information systems.

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. In addition, the Office of Inspector General provides audit reports to the Congress.

This report is intended for the information of management of the Department of the Interior, the Office of Management and Budget, and the Congress. However, this report is a matter of public record, and its distribution is not limited.

SUMMARY OF RECOMMENDATIONS AND CORRECTIVE ACTIONS FOR THE DECEMBER 1999 AUDIT REPORT "GENERAL AND APPLICATION CONTROLS OVER AUTOMATED INFORMATION SYSTEMS, OFFICE OF SURFACE MINING RECLAMATION AND ENFORCEMENT" (No. 00-I-138)

Recommendations	Status of Recommendations and Corrective Actions
A.1. Determine the risks associated with each of the systems and, based on the results of the risk assessments, establish appropriate security policies and procedures.	Implemented.
A.2. Ensure that risk assessments are conducted in accordance with Federal guidelines which recommend that risk assessments support the acceptance of risk and the selection of appropriate controls. Specifically, the risk assessments should address significant risks affecting sensitive systems and major applications, appropriately identify controls implemented to mitigate those risks, and formalize the acceptance of residual risk.	Implemented.
A.3. Formally assign and communicate responsibility to those individuals required to participate in assessing risks.	Implemented.
B.1. Provide resources to ensure that automated information systems security plans are developed for the OSM's general support systems and major applications in accordance with the Computer Security Act; Office of Management and Budget Circular A-130, Appendix III; and the National Institute of Standards and Technology's Special Publication 800-18.	Implemented.
B.2. Ensure that the automated information systems security function is elevated organizationally to report directly to the OSM's Chief Information officer and formally provide the position with the authority to implement and enforce a computer security program throughout the OSM.	Implemented.
B.3. Report the lack of security plans for the OSM's sensitive systems as a material weakness in the OSM's annual assurance statement on management controls for fiscal year 1999.	Implemented.
C.1. Ensure that personnel security policies and procedures are developed, implemented, and enforced, including those for obtaining appropriate security clearances for personnel filling sensitive or critical public trust positions.	Implemented.
C.2. Ensure that all automated data processing contractor employees have proper background clearances.	Implemented.

Recommendations	**Status of Recommendations and Corrective Actions**
C.3. Ensure that periodic reinvestigations are completed every 5 years on personnel who are in public trust high risk positions.	Implemented.
D.1. Develop and implement policies to classify the OSM's computer resources in accordance with the results of periodic risk assessments and guidance contained in Office of Management and Budget Circular A-130, Appendix III.	Implemented.
E.1. Institute a policy of "least privilege" access levels to ensure that access to resources and data is limited to those users who require such access.	Implemented.
E.2. Develop and implement policies and procedures for approving access to the automated information systems that include the formal assignment of responsibility for approving systems access.	Implemented.
E.3. Develop and implement procedures to ensure that user access levels are periodically reviewed to ensure that the current access provided is appropriate.	Implemented.
E.4. Develop and implement procedures to ensure that system administration personnel are promptly notified of changes in employee assignments or employment terminations.	Implemented.
E.5. Implement controls to ensure that system owners approve all access to their applications in accordance with the OSM's policy.	Implemented.
F.1. Develop and implement policies and procedures establishing the maximum number of log-in attempts allowed for the OSM's automated information systems in compliance with Department of the Interior regulations.	Implemented.
F.2. Ensure that the systems log-in warning message is the first screen displayed upon initial access and prior to the user being authenticated as a valid system user.	Implemented.
G.1. Develop and implement password policies and procedures. In addition, controls to ensure compliance with these policies and procedures should be implemented.	Implemented.
G.2. Implement a policy requiring system administration personnel to log on to the automated information systems under specific user IDs.	Implemented.
G.3. Evaluate current capabilities and implement procedures to address encryption or other security methods to help prevent powerful system passwords and accounts from being compromised when traveling across a network, such as the wide area network and the Internet.	Implemented.

Recommendations	**Status of Recommendations and Corrective Actions**
H.1. Develop policies and procedures to ensure that controls are in place to protect the Novell network operating system and other system software from unauthorized modification or manipulation.	Implemented.
I.1. Identify and implement the technical controls necessary to ensure that only authorized users have access to the Novell file servers. The controls should include using the "SECURE CONSOLE" command in the autoexec.ncf file, encrypting the "RCONSOLE" password, and using the "LOCK CONSOLE" command.	Implemented.
J.1. Install a firewall system for the Division of Financial Management's local area network.	Implemented.
K.1. Evaluate acquiring systems verification and auditing software.	Implemented.
K.2. Implement the systems options available in each of the operating systems to record activities affecting the systems.	Implemented.
K.3. Implement policies and procedures to ensure that systems logs are used and are maintained for an appropriate amount of time to provide an adequate audit trail of systems activities and are controlled by personnel independent of the systems access control administration function.	Implemented.
K.4. Develop and implement procedures to ensure that periodic reviews of systems logs for unauthorized or inappropriate activities are performed and that unauthorized or inappropriate activities are reported to the OSM management.	Implemented.
L.1. Establish policy and procedures for ensuring that available software updates and service packs are reviewed to identify those that should be implemented to address an applicable systems vulnerability.	Implemented.
L.2. Implement procedures to ensure that those updates which are determined to be needed are implemented in a timely manner.	Implemented.
M.1. Implement procedures to ensure that personnel who perform access control administration are not the same individuals who review and control systems security logs and systems audit trails.	Implemented.
M.2. Implement controls to ensure that application programmers are not responsible for moving changed software into the production environment and do not have access to update/change production data.	Implemented.

Recommendations	**Status of Recommendations and Corrective Actions**
N.1. Enforce OSM's written policies and procedures to ensure that all application programs and modifications are properly authorized, tested, and approved and that access to and distribution of programs is controlled.	Implemented.
N.2. Establish the process of correcting applications deficiencies as a high priority to reduce manual processes.	Implemented.
N.3. Review change requests timely to ensure that user requirements are supported in the applications.	Implemented.
O.1. Ensure that a contingency plan is developed for critical telecommunications links.	Implemented.
O.2. Ensure that contingency plans for telecommunications links, facilities, and the data center are finalized and tested and that test results are used to update these plans. Additionally, assurance should be provided that personnel are trained to implement the plans.	Partially implemented. The OSM had not completed and finalized its contingency plans or fully tested the plan for its headquarters operations.
O.3. Provide for a secure off-site storage facility that is at least 1 mile from the computer facility.	Implemented.
P.1. Develop and implement a formal incident response plan and team.	Implemented.

APPENDIX 2

United States Department of the Interior

OFFICE OF SURFACE MINING
RECLAMATION AND ENFORCEMENT
Washington, D.C. 20240

MAY 23 2001

MEMORANDUM

To: Roger LaRouche
Assistant Inspector General for Audits

Through: Piet deWitt, Acting Assistant Secretary
Lands and Minerals Management

Piet deWitt MAY 30 2001

Glenda Owens

From: Glenda Owens, Acting Director
Office of Surface Mining Reclamation and Enforcement

Subject: Draft Audit Report on Implementation of Recommendations for Improving the General Controls Over Automated Information Systems, Office of Surface Mining Reclamation and Enforcement (Assignment Number A-IN-OSM-001-00-M)

This response is to the subject Draft Audit Report on Implementation of Recommendations for Improving the General Controls over Automated Information Systems at the Office of Surface Mining (OSM).

The audit was conducted to determine whether OSM had satisfactorily implemented the 38 recommendations from the December 1999 audit report titled "General and Application Controls Over Automated Information Systems, Office of Surface Mining Reclamation and Enforcement" (No. 00-I-138) and to determine whether any new recommendations were warranted. In addition, this audit supported the Office of Inspector General's opinion on the OSM's financial statements by evaluating the reliability of the general controls over automated systems that support the annual financial statements.

The Draft Audit Report concluded that the OSM had made substantial progress in correcting the weaknesses identified in the prior Audit Report and in improving the general controls over its automated information systems by implementing 29 of the 38 recommendations. Of the remaining nine recommendations, the OSM had taken actions to partially implement six, and had not taken any action to implement three of the recommendations. This response will address each of the six partially implemented recommendations, and the three recommendations which OSM has not taken any action on implementing.

If you have questions or require additional information regarding this response, please have your staff contact Donald Griffith on 202-208-2916, or by e-mail: dgriffit@osmre.gov.

Attachment

Note: ALL ATTACHMENTS NOT INCLUDED BY OFFICE OF THE INSPECTOR GENERAL.

OFFICE OF SURFACE MINING
RESPONSE TO IG AUDIT RECOMMENDATIONS
MAY 29, 2001

OSM reviewed the Draft Audit Report Number A-IN-OSM-001-00-M, and concurs with the IG conclusion that OSM has made substantial progress in correcting the weaknesses identified in the prior IG Audit Report number 00-I-138, and in improving the general controls over its automated information systems by implementing 29 of the 38 recommendations identified in the prior audit report. In addition, OSM also agrees with the IG conclusion, that of the remaining nine recommendations, the OSM has taken actions to partially implement six recommendations and has not taken the necessary actions to implement three recommendations.

The following response address both the six partially implemented recommendations and the three recommendations which OSM has not taken the necessary actions to implement:

RECOMMENDATIONS:

A.2. **Ensure that risk assessments are conducted in accordance with the Federal guidelines which recommend that risk assessments support the acceptance of risk and the selection of appropriate controls. Specifically, the risk assessments should address significant risks affecting sensitive systems and major applications, appropriately identified controls implemented to mitigate those risks, and formalize the acceptance of residual risk.**

Response: OSM concurs with the IG on this item and offers the following response:

OSM completed a risk assessment for each of its 5 mission critical systems and has established security policies and procedures. However, the assessments had not been approved my management at the time of the IG audit review. The risk assessments have now been approved by management, and copies of the approved risk assessments are at attachment I.

C.1. **Ensure that personnel security policies and procedures are developed, implemented, and enforced, including those for obtaining appropriate security clearances for personnel filling sensitive or critical public trust positions.**

Response: OSM concurs with the IG on this item and offers the following response:

OSM has developed a Security Directive (copy at attachment II), which contains personnel security policies and procedures for obtaining appropriate security clearances for personnel filling sensitive and critical trust positions. In addition, Chapter VI of the Security Directive provides guidance on how to designate position sensitivity for all

OSM positions, and the level of background investigation which should be completed on each type of position.

The office of Personnel has identified personnel in Sensitive Computer areas and their position risk designation to ensure proper clearance and background investigations are completed. However, OSM agrees with the IG that position sensitivity classifications of critical public trust positions were not always appropriately based on the duties and risks of the position, and these computer positions were re-evaluated and updated with the responsible management official.

E.3. **Develop and implement procedures to ensure that user access levels are periodically reviewed to ensure that the current access provided is appropriate.**

Response: OSM Concurs with the IG on this item and offers the following response:

OSM has included procedures in Chapter XII, Section D of the Security Directive that user access levels are periodically reviewed to ensure that access levels provided are appropriate. OSM requires that all system administrators complete a total review of all User access privileges periodically. OSM agrees with the IG finding that reviews of users' access levels were not performed on all information systems. However, to ensure that these reviews are conducted, OSM has established an Independent Security Oversight Review Team (ISORT) to audit our information systems agency wide and ensure that procedures outlined in the Security Directive, which includes reviewing access levels are being followed.

DFM's Site Information Security Officer (SISSO), issued an e-mail to all System Administrators and System Owners that a complete review of all users' access levels for all systems and platforms must be completed by May 15, 2001. This review was completed on May 15, 2001, and a copy of the e-mail is at attachment III. DFM will continue to perform these reviews periodically.

E.4. **Develop and implement procedures to ensure that system administration personnel are promptly notified of changes in employee assignments or employment terminations.**

Response: OSM concurs with the IG on this item and offers the following response:

The OSM Employee Exit Clearance Form has been updated to include a section for the supervisor of the employee being reassigned or terminated to sign. The signature will remind the supervisor of this responsibility to immediately notify the key managers and systems owners that an employee has changed his status. The OSM e-mail system has been updated to assist the supervisor with this responsibility. The supervisor only needs to send an e-mail to "Clearance" and the e-mail will automatically be routed to key managers and all system owners to ensure that the employee's access is removed from all information systems. To ensure that these procedures are fully implemented, the Office of Personnel e-mails a monthly list of separated employees to key OSM system owners, management and staff for their review.

K.3. **Implement policies and procedures to ensure that systems logs are used and are maintained for an appropriate amount of time to provide an adequate audit trail of systems activities and are controlled by personnel independent of the systems access control administration functions.**

Response: OSM concurs with the IG on this item and offers the following response:

OSM has developed policies and procedures to ensure that systems logs are used and maintained. Both the SUN and HP computers systems at DFM maintain and retains system logs for a period of six months. The audit functions on both the NT and Novell servers in Washington are enabled. However, OSM agrees with the IG's conclusion that systems logs are not controlled by Personnel independent of the systems access administration function.

To fully implement this recommendation in Washington, D.C., OSM has assigned the NT administrator to oversee the system logs for the Novell servers and assigned the Novell administrator to oversee the systems logs for the NT servers. In Denver, DFM has implemented a policy requiring that both the primary and backup system administrator review the system logs.

M.1. **Implement procedures to ensure that personnel who perform access control administration are not the same individuals who review and control systems security logs and systems audit trails.**

Response: OSM concurs with the IG on this item and offers the following response:

DFM has procedures in place to ensure that personnel who perform access control administration are not the only individuals who review and control system security logs and system audit trails. DFM has implemented procedures requiring that both the primary and backup system administrator review the system logs, and that the system owners review system audit trails.

M.2. **Implement controls to ensure that application programmers are not responsible for moving changed software into the production environment and do not have access to update/change production data.**

Response: OSM concurs with the IG on this item and offers the following response:

Due to staffing levels, DFM is unable to provide for complete separation of duties as indicated by this finding. DFM has implemented procedures for the movement of changed software into our production environment that we feel alleviates the risks associated with this finding. In the next update of our risk analysis documents, we will specifically address each of these risks, the controls in place, and the request that management approve the procedure we have established as appropriate. The Financial and Administrative Systems Team Leader has conveyed to all team leaders, system accountants, programmers, and system administrators that these procedures are to be strictly adhered to, with no exceptions. DFM will adhere to this process and obtain all signatures before software is moved into the production environment.

N.1. **Enforce OSM's written policies and procedures to ensure that all application programs and modifications are properly authorized, tested, and approved and that access to and distribution of programs is controlled.**

Response: OSM concurs with the IG on this item and offers the following response:

OSM has developed policies and procedures to ensure that all application program modifications are properly authorized, tested, approved and that access to and distribution of programs are controlled. This policy is in Chapter XII, Section H and Chapter IV, Section D of the Security Directive. To ensure that these policies are adequately enforced, OSM has established and implemented an Independent Security Officers Review Team to audit OSM's information systems agency wide and ensure that policies are being followed.

OSM agrees with the IG Report that we were not always following our own written procedures, however, the IG did agree in the exit interview that the process used at DFM for implementing system and software changes was adequate. It has been conveyed to the appropriate staff at DFM that these procedures will be strictly adhered to, with no exceptions, and all signatures must be obtained before any software is moved into a production environment.

O.2. **Ensure that contingency plans for telecommunications links, facilities, and the data center are finalized and tested and that test results are used to update these plans. Additionally, assurance should be provided that personnel are trained to implement the plans.**

Response: OSM concurs with the IG on this item and offers the following response:

OSM has and tested its Washington, D.C., Headquarters contingency plans, and made modifications to the contingency plans, where appropriate. A copy of the test plans and results are in attachment IV.

OFFICE OF SURFACE MINING
RESPONSE TO IG AUDIT RECOMMENDATIONS
JULY 3, 2001

OSM reviewed the Draft Audit Report Number A-IN-OSM-001-00-M, and has concurred with the IG conclusions that OSM has made substantial progress in correcting the prior identified weaknesses. In our last response to this Draft Audit report we neglected to comment on items listed under **Recommendations** made to the Director, OSM. Our comments are as follows:

2. **Reevaluate the appropriateness of designated sensitive or high risk positions and the respective duties and obtain the necessary security clearances for personnel filling these sensitive or critical public trust positions.**

Response: OSM concurs with the IG on this item and offers the following response:

OSM will reevaluate the appropriateness of designated sensitive or high risk positions and respective duties and obtain the necessary security clearances. The security clearance of the position with be commensurate with actual duties and access to information and systems.

3. Ensure that the OSM's established policies and procedures are followed when granting new users' access to the Applicant Violator System.

Response: OSM concurs with the IG on this item and offers the following response:

OSM will ensure that established policies and procedures are followed when granting new users' access to the Applicant Violator System. All new user access from within OSM or from the States and Tribes will have the appropriate documentation prior to the issuance of access.

4. **Establish remote-access control procedures and remote user-set parameters and strengthen the existing practices by providing added control features and required settings or document the acceptable risk in a formal (management approved) risk assessment.**

Response: OSM concurs with the IG on this item and offers the following response:

OSM is currently reviewing our remote-access procedures and will implement procedures to increase security. Remote-access guidelines for granting user access will be reviewed to keep access to an as needed basis. Current accounts have been reviewed and inactive accounts deleted.

STATUS OF AUDIT REPORT RECOMMENDATIONS

Finding/ Recommendation Reference	Status	Actions Required
1	Resolved; not implemented.	No further response to the Office of Inspector General is required. The recommendations will be forwarded to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.
2, 3, and 4	Management concurs; additional information requested.	Provide the Office of Inspector General with target dates for actions planned and titles of officials responsible for implementation.

ILLEGAL OR WASTEFUL ACTIVITIES

SHOULD BE REPORTED TO THE OFFICE OF INSPECTOR GENERAL

Internet Complaint Form Address

http://www.oig.doi.gov/hotline_form.html

Within the Continental United States

U.S. Department of the Interior
Office of Inspector General
1849 C Street, N.W.
Washington, D.C. 20240-0001

Our 24-hour
Telephone HOTLINE
1-800-424-5081 or
(202) 208-5300

TDD for hearing impaired
(202) 208-2420

Outside the Continental United States

Caribbean Region

U.S. Department of the Interior
Office of Inspector General
Eastern Division – Investigations
4040 Fairfax Drive
Suite 303
Arlington, Virginia 22203

(703) 235-9221

Pacific Region

U.S. Department of the Interior
Office of Inspector General
Guam Field Pacific Office
415 Chalan San Antonio
Baltej Pavilion, Suite 306
Agana, Guam 96911

(671) 647-6060