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

AUDIT REPORT

IMPLEMENTATION OF RECOMMENDATIONS FOR IMPROVING GENERAL CONTROLS OVER THE AUTOMATED INFORMATION SYSTEM, ROYALTY MANAGEMENT PROGRAM, MINERALS MANAGEMENT SERVICE

REPORT NO. 99-I-628
JULY 1999

A-IN-MMS-001-98-M .

United States Department of the Interior

OFFICE OF INSPECTOR GENERAL
Washington, D.C. 20240

JUL - 9 1999

AUDIT REPORT

Memorandum

To: Assistant Secretary Land and Minerals Management

From: Robert J. Williams Robert J. Williams
Assistant Inspector General for Audits

Subject: Audit Report on Implementation of Recommendations for Improving General Controls Over the Automated Information System, Royalty Management Program, Minerals Management Service (No. 99-I-628)

INTRODUCTION

This report presents the results of our audit of implementation of the recommendations contained in our March 1998 audit report titled "General Controls Over the Automated Information System, Royalty Management Program, Minerals Management Service" (No. 98-I-336). The objective of our current audit was to determine whether the Minerals Management Service's Royalty Management Program satisfactorily implemented the recommendations made in our March 1998 report and whether any new recommendations were warranted. This audit supports the Office of Inspector General's opinion on the financial statements of the Minerals Management Service by evaluating the reliability of the general controls over computer-generated data that support the Royalty Management Program's portion of the financial statements.

BACKGROUND

The Minerals Management Service's Royalty Management Program is responsible for collecting and disbursing revenues of about $4 billion annually that are generated from leasing Federal and Indian lands and for collecting royalties on minerals extracted from leased lands. To aid in accomplishing its mission objectives and meeting its financial reporting requirements, the Program uses an automated information system that includes a mainframe computer, a minicomputer, and personal computers and servers which support an enterprisewide network.[1] For collecting rents and royalties, the Program uses primarily the mainframe computer. For disbursing rents and royalties, verifying collections, and reporting financial information, the Program uses all of the components of its automated information system. The Program's automated information system was operated and maintained by a contractor.

Overall system security policies for the Program are established by the Installation Information Technology Security Manager, within the Program's Systems Management Division. The contractor is responsible for providing system security administration for the mainframe computer, the minicomputers, and the enterprisewide network.

SCOPE OF AUDIT

This audit was conducted during September through November 1998 at the Royalty Management Program's Systems Management Division, located in Lakewood, Colorado. The scope of our audit included an evaluation of the actions taken by Program management to implement the 23 recommendations made in our March 1998 report and reviews of the general controls in place during fiscal year 1998. To accomplish our objective, we interviewed Program and contractor personnel, reviewed system documentation, and reviewed and tested implementation of the recommendations contained in the March 1998 report.

The audit was conducted in accordance with the "Government Auditing Standards," issued by the Comptroller General of the United States. Accordingly, we included such tests of records and other auditing procedures that were considered necessary under the circumstances.

As part of our audit, we evaluated the Program's general controls over its automated information system that could adversely affect the data processing environment. Because of inherent limitations in any system of internal controls, losses, noncompliance, or misstatements may occur and not be detected. We also caution that projecting our evaluations to future periods is subject to the risk that controls or the degree of compliance with the controls may diminish.

RESULTS OF AUDIT

Regarding the March 1998 report's 23 recommendations, we found that the Royalty Management Program had satisfactorily implemented 20 recommendations. Three recommendations (Nos. D. 1, D.2, and G. 1) were considered resolved but not implemented based on actions to be taken by the Program. Appendix 2 lists all of the prior report's

[1] Servers are computers that provide services to client computers on a network. Enterprisewide networks are networks that result when all the networks in a single organization are connected. (Jerry Fitzgerald and Alan Dennis, Business Data Communications and Networking, 5th edition, John Wiley & Sons, Inc., 1996.)

recommendations, the status of the recommendations, and actions taken to implement the recommendations. The actions taken on the recommendations have improved the general controls in the areas of security program, access controls, software development and change management, separation of duties, system software controls. and service continuity.

To further strengthen the general controls, we found that improvements were needed in the areas of access controls, security planning, and continuity of operations. Office of Management and Budget circulars and National Institute of Standards and Technology publications require Federal agencies to establish and implement computer security and management and internal controls to improve the protection of sensitive information in the computer systems of executive branch agencies. Program management did not ensure that (1) computer security training was received by employees and contractor personnel and access to computer processing was limited, (2) security plans were updated appropriately, and (3) disaster recovery plans were developed in compliance with established criteria. As a result, there was an increased risk of (1) unauthorized access to, modification of, and disclosure of sensitive data; (2) ineffective security planning; and (3) loss of system availability.

Overall, we identified four weaknesses and made four new recommendations for improving general controls at the Program. We do not consider these weaknesses to be a material weakness under provisions of the Federal Managers' Financial Integrity Act. A summary of the weaknesses in the areas of access controls, security planning, and continuity of operations is provided in the paragraphs that follow, and the weaknesses and our respective recommendations are detailed in Appendix 1.

Access Controls

We found weaknesses in access controls over the Program's automated information system. These weaknesses were in the areas ofcomputer security training and logical access controls over computer processing. As a result, there was an increased risk that proprietary data maintained on the automated information system were vulnerable to unauthorized disclosure and manipulation, as well as an increased risk of disruption of service to users. We made two recommendations to address these weaknesses.

Security Planning

We found a weakness in the development and maintenance of security plans for sensitive systems. As a result, the security plans in place did not ensure that controls were established to protect information processed, transmitted, or stored in the general support system,[2] and there was an increased risk that the most appropriate and effective controls would not be

'Office ofManagement and Budget Circular A- 130, Appendix III, "Security ofFederal Automated Information Resources," defines a general support system or system to mean "an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information. data. applications, communications, and people."

identified and implemented by the Program. We made one recommendation to address this weakness.

Continuity of Operations

We found that the communication networks, which were part of the Program's general support system, were not included in the Program's disaster recovery plans. As a result, there was an increased risk that the communication nenvorks may not be recovered in the event of a disaster. We made one recommendation to address this weakness.

Minerals Management Service Response and Office of Inspector General Reply

In the May 25, 1999, response (Appendix 3) to our draft report from the Director, Minerals Management Service, the Service concurred with the four recommendations. Based on the response, we consider Recommendations A.1 and B.l resolved and implemented and Recommendations C. 1 and D.l resolved but not implemented. Accordingly, the unimplemented recommendations will be referred to the Assistant Secretary for Policy, Management and Budget for tracking of implementation (see Appendix 4).

Regarding our March 1998 report, the Service, in its May 1998 response, concurred with our classification of the prior recommendations, and we considered 20 of the 23 recommendations resolved and implemented and the remaining 3 recommendations (Nos. D. 1, D.2, and G. 1) resolved but not implemented. Accordingly, updated information on the status of the three prior unimplemented recommendations will be forwarded to the Assistant Secretary for Policy, Management and Budget (see Appendix 5).

Since the recommendations contained in this report are considered resolved, no further response to the Office of Inspector General is required (see Appendix 4).

The legislation, as amended, creating the Office of Inspector General requires semiannual reporting to the Congress on all audit reports issued. actions taken to implement audit recommendations, and identification of each significant recommendation on which corrective action has not been taken.

We appreciate the assistance of Service personnel in the conduct of our audit.

DETAILS OF WEAKNESSES AND RECOMMENDATIONS

ACCESS CONTROLS

A. Computer Security Training

Condition: The Program's policy that required periodic computer security training of employees and contractor personnel to reduce the risk of disclosure of proprietary data had not been effectively implemented. We statistically tested 49 of the 717 employees who had access to the server component of the automated information system. We found that 28 of the 49 employees had not received periodic training in the protection of proprietary data. From our test results, we projected that of the 717 employees, 410 employees had not been trained recently in the protection of proprietary data. In addition, Program management did not ensure that contractor personnel received such training.

Criteria: The Program's policy regarding data protection states that the Royalty Management Program will "rely on employee training, clearances, and physical controls as its primary means ofprotecting proprietary information." This policy also states that "all employees and contractors are required to protect proprietary information and receive periodic training regarding the protection of proprietary information."

Cause: There were no controls in place to ensure that employees and contractor personnel received the training specified by Program policy.

Effect: Since training was one of the Program's primary controls to protect against disclosure of proprietary data and this control had not been effectively implemented, there was an increased risk of unauthorized disclosure of proprietary data.

Recommendation:

We recommend that the Director, Minerals Management Service, implement procedures to ensure that all employees and contractor personnel receive periodic training on the protection of proprietary data as defined by Program policy.

ACCESS CONTROLS

B. Access Controls Over Computer Processing

Condition: Access controls over the processing performed on the mainframe computer were inadequate. Specifically, we identified 171 individuals who had update access to the emergency libraries.[1] Emergency libraries can contain changes to the production application programs that are used to process data to determine the distribution of royalties. By running a program from the emergency library, change control procedures are bypassed, and the risk is increased that an inappropriate program would be run which could adversely affect the Program’s data.

Criteria: Office of Management and Budget Circular A-130, Appendix III, “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. The Circular also requires agencies to implement and maintain a program to ensure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. The Circular further defines “adequate security” as “security commensurate with the risk and the magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information.” In addition, the current Program policy addressing data protection states that the Program “applies the concept of ‘least privilege’ to protect the integrity of official records. Only those persons with the responsibility for adding, deleting, or modifying records are given update privileges.”

Cause: Program security administration personnel had established a group within the mainframe computer security software that included all Time Sharing Option’ (TSO) users and had given this group update access to the emergency

“‘A library is a collection of programs or data files for a particular purpose.” (Alan Freedman, The Computer Glossary, 4th edition. AMACOM Division of the American Management Association, 1989, p. 401.)

[2]Time Sharing Option is a software “that provides interactive communications for IBM’s MVS [Multiple Virtual Storage] operating system. It allows a user or programmer to launch an application from a terminal and interactively work with it.” MVS is the operating system used on IBM mainframes. “MVS is a batch processing-oriented operating system that manages large amounts of memory and disk space. Online operations are provided with CICS [Customer Information Control System], TSO and other system software.” (Computer Desktop Encyclopedia, Version 9.4, 4th quarter, 1996, The Computer Language Company, Inc.)

ACCESS CONTROLS

libraries, even though all users with access to TSO were not authorized to perform updates to the emergency libraries. Although Program management relied on reviews by personnel responsible for managing changes and updates to the emergency libraries to detect any inappropriate activities, we believe that a more effective control would have been to reduce the possibility of inappropriate activities by limiting access.

Effect: There was an increased risk that unauthorized changes to the mainframe applications in the production environment could occur, which could result in possible corruption[3] and loss of data, as well as disruption of service to users. However, during our fieldwork, the Program eliminated the update access to the emergency libraries that was provided to all TSO users.

Recommendation:

We recommend that the Director, Minerals Management Service, establish policies and procedures to ensure that default accesses established in the automated information system provide access only to authorized users requiring such access.

‘Corruption is the unauthorized altering of data or programs resulting in erroneous software logic. (Alan Freedman, The Computer Glossary, 4th edition, AMACOM Division of the American Management Association, 1989, p. 159.)

SECURITY PLANNING

C. Security Plans

Condition: The security plans for sensitive systems referred to in the Program's "Automated Information Systems Security Plan," dated January 1998, did not reflect the current information technology environment at the Program. Specifically, the "IBM Security Plan" and the "DECNAX [Digital Equipment Corporation/Virtual Address Extension] Security Plan" were dated 1996. The IBM plan did not reflect the hardware platform that was implemented in 1997. Further, both of the plans identified the Outer Continental Shelf Information System (OCSIS) as a source of production information, but OCSIS had been replaced by the Technical Information Management System. Also, the "RMP Desktop 1997 Security Plan" identified the Resource Access Control Facility (RACF) and the System Management Facility (SMF) as the audit and variance detection controls in place. However, both RACF and SMF were in place on the mainframe, but the Royalty Management (RMP) Desktop application was a client/server system, that used different audit and variance detection controls.

Criteria: The Computer Security Act of 1987 requires the development of a security plan for each Federal computer system that contains sensitive information. The Act further states, "Such plan shall be revised annually as necessary." Office of Management and Budget Circular A-130, Appendix III, "Security of Federal Automated Information Resources," requires that security plans be developed for each general support system. In addition, the Departmental Manual (375 DM 19) requires that security plans be prepared for new or significantly changed systems.

Cause: Program management updated only the plans that were referred to in the Program's "Automated Information Systems Security Plan" every 3 years regardless of whether changes had occurred. In addition, Program management did not ensure that the Program's security plans accurately reflected the security controls of the Program's sensitive systems components.

Effect: Security plans for the Program did not ensure that controls were established to protect information processed, transmitted, or stored in the general support system, and there was an increased risk that the most appropriate and effective general controls would not be identified and implemented by the Program. During our fieldwork, Program security management revised the

SECURITY PLANNING

IBM plan, “Mainframe - 1998 Security Plan,” to reflect the current mainframe environment.

Recommendation:

We recommend that the Director, Minerals Management Service, ensure that security plans which are referred to in the Program’s annual “Automated Information System Security Plan” accurately reflect the controls in place and are updated to reflect significant changes to the current information technology environment.

CONTINUITY OF OPERATIONS

D. Disaster Recovery Plans

Condition: Communication networks, which are part of the Program's general support system, used by the Program's divisions that maintain proprietary and financial data were not included in the Program's disaster recovery plans.

Criteria: Office of Management and Budget Circular A- 130 requires that the security plan for a general support system address continuity of operations. The Circular states, "Agency plans should assure that there is an ability to recover and provide service sufficient to meet the minimal needs of users of the system. Manual procedures are generally NOT a viable back-up option."

Cause: Program management had not completed the Program's disaster recovery plan for its communication network environment.

Effect: If the disaster recovery plans are incomplete because components of the general support system are not included, personnel required to perform the disaster recovery procedures may not be able to recover critical systems in the event of a disaster or a system failure.

Recommendation:

We recommend that the Director, Minerals Management Service, ensure that disaster recovery plans are developed for the general support system, including communication networks necessary to maintain Program operations.

SUMMARY OF RECOMMENDATIONS AND CORRECTIVE ACTIONS FOR AUDIT REPORT "GENERAL CONTROLS OVER THE AUTOMATED INFORMATION SYSTEM, ROYALTY MANAGEMENT PROGRAM, MINERALS MANAGEMENT SERVICE" (No. 98-I-336)

Recommendations	**Status of Recommendations and Corrective Actions**
A.1. Ensure that risk assessments are conducted in accordance with guidelines which recommend that risk assessments support the acceptance of risk and the selection of appropriate controls. Specifically, the assessments should address significant risks affecting systems, appropriately identify controls implemented to mitigate those risks, and formalize the acceptance of the residual risk.	Implemented. We found that the Royalty Management Program had implemented an enhanced risk assessment process which should identify the significant risks affecting the Program's automated information system, identify controls implemented to mitigate those risks, and formalize the acceptance of the residual risk. We believe that establishment of this process meets the intent of the recommendation.
A.2. Formally assign and communicate responsibility to local area network administrators to participate in risk assessments and ensure compliance with the Program's security policy.	Implemented. The Program had centralized the administration of its networks and established a team to ensure compliance with the Program's policy regarding risk assessments.
A.3. Determine the risks associated with local area network applications and personal computer databases which contain proprietary and financial data and, based on the results of the risk assessments, establish appropriate security policies and procedures.	Implemented. The Program had performed an assessment of risks related to proprietary data and its official financial records. As a result of the assessment, the official records had been moved from personal computer databases to networks. Therefore, the proprietary and official financial records are subject to the controls established for the networks.

Recommendations	Status of Recommendations and Corrective Actions
B. 1. Evaluate Systems Management Division and contractor automated data processing (ADP) positions to determine position sensitivity in relation to risk and ADP factors. Also, assurance should be provided that automated information system work is technically reviewed by persons whose position sensitivity levels are greater than the position sensitivity levels of the employees who are performing the work.	Implemented. The Program had evaluated Systems Management Division and contractor ADP positions to determine position sensitivity in relation to risk and ADP factors. Through the evaluation process, the sensitivity levels of Systems Management Division management and supervisory positions and contractor management positions were increased.

Recommendations	Status of Recommendations and Corrective Actions
B.2. Establish controls to ensure that the contractor is fulfilling its contractual obligation of submitting requests for background checks within the specified time frame and that contractor employees who are in probationary status and awaiting security clearances are not performing critical ADP work.	Implemented. A process was implemented in which the contractor provided a report containing the names of newly hired personnel working on the Program's contract, along with the submission status of the background check documentation. This report was used by the Program's security management and the Minerals Management Service's Personnel Division to ensure compliance with contract requirements regarding the submission of background check documentation. Also, the Program approved the contractor's implementation of a "pre-employment/pre-assignment screening" process. This process, which includes a criminal history review, credit check, and a driving history check, provides assurance to the Program that the contractor's potential employees would receive the appropriate security clearance. This procedure was implemented in lieu of not allowing contractor employees who are on probationary status and awaiting their security clearances to perform critical ADP work because the time required to obtain a security clearance is not cost beneficial to the Program. We believe that the contractor's alternative "pre-employment/pre-assignment screening" process meets the intent of the recommendation.

Recommendations	Status of Recommendations and Corrective Actions
B.3. Establish controls to ensure that personnel or security files accurately reflect that background checks and periodic followup background checks are performed as required.	Implemented. Program background check information was being tracked by the Service's Personnel Division for Program and contractor personnel instead of requests for background checks being submitted through the Program's security personnel. In addition, Program management had taken action to submit required documentation for periodic followup background checks.
C. 1. Establish controls to enforce Program policy that requires employees to sign security awareness statements before access to system resources is approved by the Installation Automated Information System Security Officer.	Implemented. The controls were established and enforced.
D. 1. Ensure that individual computer resources are classified based on the level of sensitivity associated with each resource.	Resolved; not implemented. Although Program management did not agree with the recommendation in its response to our March 1998 audit report, we believe that the Program's risk management process implemented under Recommendation A. 1 will require the Program to classify its individual computer resources based on the level of sensitivity associated with each resource. Therefore, we believe that completion of the revised risk assessments, which the Service said will occur by the end of calendar year 1999 using the new risk management process, will meet the intent of the recommendation.

Recommendations	Status of Recommendations and Corrective Actions
D.2 Evaluate controls over resources to ensure that the access controls have been implemented commensurate with the level of risk and sensitivity associated with each resource.	Resolved; not implemented. Although Program management did not agree with the recommendation in its response to our March 1998 audit report, we believe that the Program's risk management process being implemented under Recommendation A. 1 will require the Program to evaluate its controls over its resources to ensure that the access controls have been implemented commensurate with the level of risk and sensitivity associated with each resource. Therefore, we believe that completion of the revised risk assessments, which the Service said will occur by the end of calendar year 1999 using the new risk management process, will meet the intent of the recommendation.
E. 1. Implement controls to enforce Program policy that default user identifications (IDs) and passwords are removed from the automated information system when commercial off-the-shelf software is implemented.	Implemented. Program management issued a memorandum reaffirming the Program's policy, and a procedure requiring assurance of deletion/revocation of the default password was implemented.

Recommendations	Status of Recommendations and Corrective Actions
F. 1. Evaluate the current Program policy which recommends that passwords contain a mix of letters and numbers for all automated information system components. Implement, if the Program determines that a mix of letters and numbers should be required, the security software option within RACF (Resource Access Control Facility) that would enforce this requirement. If the Program determines that a mix of letters and numbers is not required, the risk should be addressed in the risk assessment.	Implemented. The Program evaluated the current policy. As a result of the evaluation, the Program implemented a control within the mainframe environment requiring the use of passwords containing a mix of letters and numbers.
F.2. Develop and implement centralized security administration for the local area networks used by the Program's divisions that contain proprietary and financial data.	Implemented. The Program consolidated its servers and centralized security administration for its local area networks that contain proprietary or financial data.
G. 1. Implement controls to ensure that access managers approve all access to their applications in accordance with Program policy.	Partially implemented. The Program made significant progress in completing its review of user access levels; however, the September 30, 1998, target date for implementation of this recommendation was changed to June 30, 1999.
G.2. Document procedures which require that users' access levels be reviewed periodically or that employees be recertified to ensure that the levels of access granted are appropriate for the duties assigned to the users.	Implemented. Procedures were documented, and the Program had begun to review user access levels cited in Recommendation G. 1.

Recommendations	Status of Recommendations and Corrective Actions
H. 1. Evaluate the need to deviate from the Department of the Interior standard for the number of unsuccessful log-in attempts. If the Program determines that this number should remain at five, Program management should request, from the Department, a waiver from the standard of three attempts.	Implemented. The Department's Office of Information Resources Management provided a waiver to the Program allowing the program to deviate from the standard pertaining to the number of log-in attempts.
I. 1. Enforce procedures for authorizing, approving, and testing client/server applications software before the software is moved into production.	Implemented. The Chief, Systems Management Division, issued a memorandum reinforcing the established procedures, and a monitoring officer was designated to ensure compliance with the standards on all new client/server projects.
J. 1. Implement controls to ensure that application programmers do not have access to the production client/server application data or the capability to update/change these data.	Implemented. Controls were established to provide only temporary access in cases in which application programmers need to access production data and to promptly terminate this access when it is no longer required.
5.2. Improve detection controls by ensuring that management or the Installation Security Officer periodically reviews server security log files.	Implemented. Procedures were developed and implemented requiring periodic reviews of server security logs by security administration personnel.
K. 1. Ensure that the upgraded version of RACF is implemented immediately if the Program is granted a waiver from consolidating its mainframe operations with another mainframe operation.	Implemented. The upgraded version of RACF was implemented.

Recommendations	Status of Recommendations and Corrective Actions
L. 1. Evaluate acquiring system verification and auditing software.	Implemented. The Program completed an evaluation of system verification and audit software and purchased a software tool to be used in its network environment that would include the mainframe.
L.2. Implement the system options to record activities in the system log (SYSLOG) during the system initialization process and develop and implement procedures to ensure that periodic reviews of the SYSLOG for unauthorized or inappropriate activities are performed and that unauthorized or inappropriate activities are reported to Program management.	Implemented. In fiscal year 1998, the Program implemented system options to record activities in the SYSLOG during the system initialization process and developed and implemented procedures requiring periodic reviews of the SYSLOG for unauthorized or inappropriate activities and requiring that such activities be reported to Program management. However, during this audit, we noted that the system logging option was disabled. After we informed Program management of this deficiency, the system logging option was turned back on.
L.3. Evaluate the available System Management Facility (SMF) record types and implement procedures to ensure that critical SMF log files are reviewed periodically and that Program management addresses the problems identified.	Implemented. The Program performed an evaluation of the record types and established procedures requiring periodic reviews of those record types that were determined to be critical.
M. 1. Update the disaster recovery plans to include all mission-critical systems.	Implemented. Program management evaluated its systems and determined that only those systems on the mainframe were mission critical. The Program had a disaster recovery plan in place to address mainframe system recovery.

United States Department of the Interior

MINERALS MANAGEMENT SERVICE
Washington, DC 20240

150
U.S. Department of the Interior
1849•1999

MAY 25 1999

Memorandum

To: Assistant Inspector General for Audits

Through: acting for Sylvia V. Baca MAY 24 1999
Acting Assistant Secretary for Land and Minerals Management

From: ~~Walt~~ Acting Rosenbusch Lucy Querques Denett
Director, Minerals Management Service

Subject: Office of Inspector General Draft Audit Report, "Implementation of Recommendations for Improving General Controls Over the Automated Information System, Royalty Management Program, Minerals Management Service" [A-IN-MMS-001-980M]

We appreciate the opportunity to respond to this draft report on our implementation of recommendations to improve the general controls over our automated information system. As outlined in your report, we have implemented 20 of the 23 recommendations and are in the process of implementing the remaining 3 recommendations. We agree with the four additional recommendations in this report and plan to implement them this year.

We're sending you our general comments on the audit findings and specific ones on the recommendations.

Please contact Bettine Montgomery at (202) 208-3976 if you have any further questions.

Attachment

' MINERALS MANAGEMENT SERVICE RESPONSE TO DRAFT AUDIT REPORT "IMPLEMENTATION OF RECOMMENDATIONS FOR IMPROVING GENERAL CONTROLS OVER THE AUTOMATED INFORMATION SYSTEM, ROYALTY MANAGEMENT PROGRAM, MINERALS MANAGEMENT SERVICE"

Audit Agency: Office of Inspector General (OIG)

Audit Number: A-IN-MMS-001-98-M

We appreciate the opportunity to review this draft report summarizing OIG's followup on the 23 recommendations contained in its March 1998 audit report, "General Controls Over the Automated Information System, Royalty Management Program, Minerals Management Service." We agree with the status shown for those recommendations. Twenty have been implemented, one will be implemented by June 1999, and the other two will be implemented via alternative approaches by the end of this calendar year. As explained in our response to the March 1998 report, we do not agree with a number of the adverse conclusions on which the recommendations were based. However, we do agree that our implementation of these recommendations will improve our general controls.

This draft report presents four additional recommendations to strengthen system access controls, security planning, and continuity of operations. We agree with each of these recommendations and are working to implement them as discussed below.

Recommendation A 1. *Implement procedures to ensure that all employees and contractor personnel receive periodic training on the protection ofproprieta y data as defined by Program policy.*

Agree. The Royalty Management Program (RMP) has provided annual training in this area, but has not enforced attendance. Because staff turnover has been minimal, we believe most employees are fully aware of the proprietary information protection requirements. Nevertheless, RMP will provide mandatory security training, including training on the protection of proprietary data, during the fall of 1999 and at least biannually thereafter. Procedures to guide this training effort will be in place by June 30, 1999.

Recommendation B 1. *Establish policies and procedures to ensure that default accesses established in the automated information system provide access only to authorized users requiring such access.*

Agree. OIG noted that all Time Sharing Option (interactive) users had update access to the "emergency library" of programs which could possibly result in unauthorized changes to the code. Our contractor' s security personnel have already corrected this problem limiting such access to the few users who need it. Documented policy and procedures will be in place by May 31, 1999.

Recommendation C 1. *Ensure that security* **plans** *which are referred to in the Program 's annual Automated Information System Security Plan accurately reflect the controls in place and are updated to reflect significant changes to the current information technology environment.*

Agree. The security plans are being updated concurrently with various ongoing system changes such as conversion of RMP 's solid minerals production accounting programs to the mainframe environment. They will be completed and in place by October 1, 1999.

Recommendation D 1. *Ensure that disaster recovery plans are developedfor the general support system, including communication networks necessary to maintain Program operations.*

Agree. RMP is working with its operations and maintenance contractor to develop such plans which will be in place by September 30, 1999.

The Chief, Systems Management Division, is responsible for implementing these recommendations.

STATUS OF CURRENT AUDIT REPORT RECOMMENDATIONS

Finding/Recommendation Reference	Status	Action Required
A.1 and B.l	Implemented.	No further action is required.
C.l and D.l	Resolved; not implemented.	No further response to the Office of Inspector General is required. The recommendations will be referred to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.

APPENDIX 5

STATUS OF PRIOR AUDIT REPORT RECOMMENDATIONS

Finding/Recommendation Reference	Status	Action Required
A.1, A.2, A.3, B.l, B.2, B.3, C.1, E.1, F.1, F.2, G.2, H.l, 1.1, J.l, 5.2, K.l, L.l, L.2, L.3, and M.l	Implemented.	No further action is required.
D.1, D.2, and G.1	Resolved; not implemented.	No further response to the Office of Inspector General is required. The information regarding the status of these recommendations will be provided to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.

ILLEGAL OR WASTEFUL ACTIVITIES SHOULD BE REPORTED TO THE OFFICE OF INSPECTOR GENERAL

Internet/E-Mail Address

www.oig.doi.gov

Within the Continental United States

U.S. Department of the Interior
Office of Inspector General
1849 C Street, N.W.
Mail Stop 5341
Washington, D.C. 20240

Our 24-hour
Telephone HOTLINE
I-800-424-508 1 or
(202) 208-5300

TDD for hearing impaired
(202) 208-2420 or
1-800-354-0996

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

North Pacific Region

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

(671) 647-6060

Toll Free Numbers:
I-800-424-5081
TDD l-800-354-0996

FTS/Commercial Numbers:
(202) 208-5300
TDD (202) 208-2420

HOTLINE

1849 C Street, N.W.
Mail Stop 5341
Washington, D.C. 20240