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

AUDIT REPORT

GENERAL AND APPLICATION CONTROLS OVER THE TECHNICAL INFORMATION MANAGEMENT SYSTEM, OFFSHORE MINERALS MANAGEMENT, MINERALS MANAGEMENT SERVICE

REPORT NO. 00-I-647
AUGUST 2000

EXECUTIVE SUMMARY

General and Application Controls Over the Technical Information Management System, Offshore Minerals Management, Minerals Management Service
Report No. 00-I-647
August 2000

BACKGROUND

The Minerals Management Service (MMS) manages the Nation's natural gas, oil, and other mineral resources on the Outer Continental Shelf and collects, accounts for, and disburses revenues from offshore and onshore mineral leases on Federal and Indian lands. MMS's Offshore Minerals Management (OMM) program manages the Outer Continental Shelf mineral leases. These leases result in more than $4 billion of royalties being collected annually. Also, OMM provides oversight to ensure safe and environmentally sound exploration and production of the Nation's mineral resources on the Outer Continental Shelf. To accomplish its mission and to automate business and regulatory functions, OMM designed, developed, and implemented the Technical Information Management System (TIMS), an MMS mission-critical system and a comprehensive corporate database.

OBJECTIVE

The objective of the audit was to determine whether OMM had effective general and application controls over TIMS and whether TIMS was operated in compliance with applicable Federal laws and regulations. In addition, we performed this audit to support the Office of Inspector General's examination of the financial statements of MMS by evaluating the reliability of the controls over computer-generated data that support the Royalty Management Program's portion of the financial statements.

RESULTS IN BRIEF

Overall, we concluded that OMM had established adequate general and application controls over TIMS. However, improvements are needed in four areas in OMM's general and application controls over TIMS. These areas are the security program, the continuity of operations plan to protect data in the event of a disaster or a system failure, controls over access to TIMS data, and software development and change management. Federal laws and regulations and Department of the Interior and MMS policies and procedures require that general and application controls be established and implemented to protect information in computer systems. Weaknesses existed in the controls over TIMS because OMM management had not developed an adequate security program and had not ensured that policies and procedures were followed. The lack of adequate controls increased the risk that TIMS data could be accessed and modified or disclosed by unauthorized users, that TIMS software and data could be stolen or destroyed, that TIMS functions and processes could not be recovered in the event of a disaster or a system failure, and that TIMS could not perform as intended.

RECOMMENDATIONS

We made 15 recommendations related to MMS's controls over TIMS. These recommendations related to improving (1) OMM's security program over TIMS, (2) TIMS' continuity of operations plan, (3) access controls to TIMS and its databases, and (4) the policies and procedures for making changes to TIMS software and for testing the changes.

AUDITEE COMMENTS AND OIG EVALUATION

MMS concurred with the report's 15 recommendations. Based on the response, we considered eight recommendations resolved and implemented and seven recommendations resolved but not implemented.

United States Department of the Interior

OFFICE OF INSPECTOR GENERAL
Washington, D.C. 20240

AUG 31 2000

AUDIT REPORT

Memorandum

To: Director, Minerals Management Service

From: Roger La Rouche Roger LaRouche
Acting Assistant Inspector General for Audits

Subject: Audit Report on General and Application Controls Over the Technical Information Management System, Offshore Minerals Management, Minerals Management Service (No. 00-I-647)

INTRODUCTION

This report presents the results of our review of general and application controls over the Minerals Management Service's (MMS) Technical Information Management System (TIMS). The objective of the audit was to determine whether MMS had effective controls over TIMS and whether TIMS was operated in compliance with applicable Federal laws and regulations. In addition, we performed this audit to support the Office of Inspector General's examination of the financial statements of MMS by evaluating the reliability of the controls over computer-generated data that support the Royalty Management Program's portion of the financial statements.

BACKGROUND

MMS manages the Nation's natural gas, oil, and other mineral resources on the Outer Continental Shelf and collects, accounts for, and disburses revenues from offshore and onshore mineral leases on Federal and Indian lands. In 1998, MMS collected $5.6 billion from Federal and Indian mineral leasees, of which $4.3 billion was from Outer Continental Shelf mineral leasees. MMS has two specialized operating programs, the Offshore Minerals Management (OMM) program and the Royalty Management Program. OMM manages the Outer Continental Shelf mineral leases and provides oversight to ensure the safe and environmentally sound exploration and production of the Nation's mineral resources on the Outer Continental Shelf. OMM has its headquarters in Washington, D.C., with offices in Herndon, Virginia, and has regional offices in New Orleans, Louisiana; Anchorage, Alaska; and Camarillo, California. Also, the headquarters OMM Leasing Division has its Mapping and Boundary Branch, located in Denver, Colorado. The Royalty Management Program manages the accounting for and the collection and disbursement of royalty, rent, and bonus revenues generated from Federal and Indian mineral leases.

To accomplish its mission, OMM designed, developed, and implemented TIMS, an MMS mission-critical system and a comprehensive corporate database that replaced and upgraded all Federal information processing resources which supported the OMM program. TIMS was developed to modernize and replace several critical offshore systems, including the Outer Continental Shelf Information System, the Offshore Inspection System, the Automated Cartographic System, and the Geological and Geophysical Database. TIMS information is used, in part, to update the Royalty Management Program system with oil and gas well production data from offshore leases to assist in verifying the accuracy of royalties collected from the Outer Continental Shelf.

TIMS is a computerized information system that automates all business and regulatory functions of OMM. TIMS is a three-tier[1] client/server platform with application servers located at all the OMM regional offices (three) and district offices (six) and database servers located at the regional offices. The Chief of the OMM Information Technology Division is the owner of TIMS. The Division is responsible for developing and maintaining TIMS's database structures, and regional and district offices are responsible for the data in the databases. TIMS employs the Oracle relational database management system and tools to manage data and support OMM business functions. In addition, TIMS includes commercial off-the-shelf software for OMM geologic interpretative tools and mapping functions. TIMS is constructed of 41 business components[2] (the components are listed in Appendix 2), which include more than 800 modules. To operate, TIMS uses approximately 55 different types of hardware items, such as personal computers and network equipment, and 68 software items, such as Windows NT and UNIX operating systems, ArcView, Geoquest, and Microsoft Office.

SCOPE OF AUDIT

We reviewed OMM general and application controls over TIMS. Specifically, we reviewed the following general controls: (1) software development and change management, (2) risk assessment, (3) security plans, (4) service continuity, (5) system software, and (6) access controls. For application controls, we reviewed input, processing, authorization, and output.

[1] A three-tier client/server environment is defined as one in which "the user interface is stored in the client, the bulk of the business application logic is stored in one or more servers, and the data are stored in a database server." (The Computer Language Company, Inc., Computer Desktop Encyclopedia, 1981-1999)

[2] TIMS is divided into major groupings or components that correspond to the different activities overseen by OMM.

To accomplish our objective, we interviewed OMM and contractor personnel, reviewed application and systems documentation, observed and became familiar with system operations and data structures, analyzed access and security controls, and evaluated service continuity procedures and testing. The audit was conducted at the Information Technology Division Office of OMM and the OMM Gulf of Mexico Regional Office in New Orleans and Division headquarters and the Information Management Division in Herndon. Although TIMS is installed at all of the regional offices, our review was limited to the Gulf of Mexico Regional Office because this regional office processes almost 90 percent of the data related to oil and gas production and Outer Continental Shelf royalties.

Our audit was made 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 employed statistical test samples to determine the adequacy of TIMS access controls and software development and change management procedures. Specifically, we randomly selected 77 TIMS users from a list of 849 users who had access to TIMS. Also, we randomly selected 132 change requests from a list of 1,157 change requests for the period of October 1998 through June 1999.

During our audit, the Department of the Interior's Office of Information Resources Management contracted to acquire professional services to support the Department with testing, analysis, and vulnerability assessment of Departmentwide information technology architecture. Specifically, the contractor was tasked with performing a comprehensive vulnerability analysis (using Internet Security Systems scanning software) of Departmental internet protocol address assignments, which included OMM internet protocol addresses. As a result, we did not review the results of the analysis of OMM networks.

PRIOR AUDIT COVERAGE

During the past 5 years, neither the General Accounting Office nor the Office of Inspector General has issued any reports related to OMM's general and application controls over TIMS.

RESULTS OF AUDIT

We concluded that overall, MMS's OMM had established adequate general and application controls over TIMS. However, we believe that the general controls of OMM need improvements in four areas: security program; continuity of operations in the event of a disaster or a system failure; controls over access to TIMS; and software development and change management. Office of Management and Budget Circular A-130, "Management of Federal Information Resources," and National Institute of Standards and Technology publications and guidelines require agencies to establish and implement computer security and management and internal controls to improve the protection of sensitive[3] information in the computer systems of executive branch agencies. Additionally, the Congress enacted laws, such as the Privacy Act of 1974 (5 U.S.C. § 552a) and the Computer Security Act of 1987 (40 U.S.C. § 759), to improve the security and privacy of sensitive information in computer systems by requiring executive branch agencies to ensure that the level of computer security and controls over sensitive information is adequate. Further, the Department of the Interior and MMS have issued policies and procedures to implement general and application controls to protect sensitive data in automated information systems. Weaknesses existed in the general controls over TIMS because OMM management had not developed an adequate security program and had not ensured that policies and procedures were followed. The lack of adequate controls may increase the risk of (1) unauthorized access and modifications to and disclosure of sensitive TIMS data, (2) theft or destruction of OMM software and sensitive information, (3) loss of TIMS systems and functions in the event of a disaster or a system failure, and (4) TIMS not performing as intended.

In the four areas that needed improvements in the controls, we identified 8 weaknesses and made 15 recommendations for improving the controls over TIMS. The weaknesses are summarized in the paragraphs that follow, and details of the weaknesses and our respective recommendations to correct these weaknesses are in Appendix 1.

Security Program

OMM management did not have a security plan for TIMS and did not ensure that computer security awareness training was provided. As a result, there was an increased risk that sensitive data could be impaired or compromised and that data could be inadvertently disclosed or destroyed or erroneously modified. We made three recommendations to correct these weaknesses.

Service Continuity

OMM's contingency planning, backup, and disaster recovery procedures did not provide reasonable assurance that the TIMS processing environment could be recovered in the event of a disaster or a system failure. Specifically, the Continuity of Operations Plan had not been tested, critical personnel had not been trained to effectively implement the Plan, a copy of the Plan was not kept at the off-site storage facility, and TIMS data and applications were not routinely transferred to the off-site storage facility. As a result, there was an increased risk that the mission-critical TIMS could not be recovered in the event of a disaster or a system failure. We made five recommendations to address these weaknesses.

[3] "Sensitive data" is defined in 40 U.S.C. § 759 as "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act)."

Access Controls

OMM management did not limit the numbers of log-in attempts allowed for access to TIMS, did not control password settings, did not remove in a timely manner access for employees who terminated their employment, and did not control access to TIMS databases. As a result, there was an increased risk that sensitive data maintained on TIMS were vulnerable to unauthorized access, manipulation, and disclosure. We made four recommendations to address these weaknesses.

Software Development and Change Management

OMM management did not implement controls to ensure that TIMS application software changes were authorized, approved, and tested before being moved into production. As a result, there was an increased risk that TIMS applications may not perform as intended. We made three recommendations to address these weaknesses.

MMS Response and Office of Inspector General Reply

In the July 19, 2000 response (Appendix 3) to the draft report from the Director of MMS, MMS concurred with all of the 15 recommendations. Based on the response, we consider Recommendations C.1, C.3, C.4, D.1, D.2, E.1, F.1, and G.1 resolved and implemented and Recommendations A.1, B.1, B.2, C.2, C.5, G.2, and H.1 resolved but not implemented. Accordingly, the unimplemented recommendations will be forwarded to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.

Although MMS concurred with Recommendation H.1, it disagreed with the "analysis that drew the auditors to the recommendation." MMS stated that although the TIMS Maintenance Methodology required test plans, the test plans were not required for "routine and/or minor changes," such as reports, system administration functions, database triggers, software packages, and menu changes. We believe that testing is a critical component of software maintenance because testing ensures that applications meet user and management needs, produce reliable data, and operate in accordance with laws, regulations, and management policies and procedures. Test plans should define the expected output and include tests for valid, invalid, expected, and unexpected results. The TIMS Maintenance Methodology does not allow for exceptions from change management procedures such as testing for system administration, database triggers, software packages, and menu changes. Further, the TIMS Maintenance Methodology does not allow for exceptions to exclude the quality assurance group and user group from testing changes prior to the changes being moved into production. The Methodology states that "every TIMS work product must pass quality assurance tests before made available for testing by the Customer User Acceptance Team."

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

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.

DETAILS OF WEAKNESSES AND RECOMMENDATIONS

SECURITY PROGRAM

A. Computer Security Plan

Condition: Offshore Minerals Management (OMM) had not developed a security plan for the Technical Information Management System (TIMS), which has been identified by the Minerals Management Service (MMS) as a sensitive and mission-critical system.

Criteria: Security plans are required by 40 U.S.C. § 759 and Appendix III, "Security of Federal Automated Information Resources," of Office of Management and Budget Circular A-130, "Management of Federal Information Resources," to be developed for all sensitive computer systems. A computer security plan is designed to assist agencies in addressing the protection of general support systems and major applications that contain sensitive information to help ensure the system's integrity, availability, and confidentiality. In addition, National Institute of Standards and Technology's (NIST) Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems," provides guidance on developing, implementing, and monitoring security plans for automated information systems. Also, Appendix III of Circular A-130 requires that a summary of the security plan be incorporated into the agency's Strategic Information Resources Management Plan. Additionally, Appendix III of Circular A-130 states that the lack of a security plan for a major application should be considered a deficiency pursuant to Office of Management Budget Circular A-123, "Management Accountability and Control," and the Federal Managers' Financial Integrity Act (31 U.S.C. § 1105, 1113, and 3512).

Cause: OMM information technology officials did not ensure that a computer security plan for TIMS was prepared in accordance with 40 U.S.C. § 759, Office of Management and Budget requirements, and NIST guidelines. According to OMM officials, a draft TIMS Y2K (Year 2000) contingency plan was prepared that addressed degradation or failure of activities and remedies should any event threaten or disable the system. However, this plan did not meet the requirements for a security plan because it did not include the rules of the system, such as rules of behavior concerning use of, security in, and acceptable level of risk for the system; training of all individuals on their security responsibilities; personnel controls; incident response

SECURITY PROGRAM

capability; continuity of support; technical security; and identification of connections to other systems.

Effect: Without this plan, OMM did not have adequate assurance that data in its TIMS were adequately protected.

Recommendation

We recommend that the Director of MMS ensure that a computer security plan for TIMS is developed, implemented, and monitored in accordance with the United States Code, Office of Management and Budget Circular A-130, and NIST guidelines.

SECURITY PROGRAM

B. Computer Security Training

Condition: Mandatory computer security awareness training had not been provided to OMM employees and contractor personnel. Specifically, at least 220 Gulf of Mexico Regional Office and district personnel and Information Technology Division personnel had not received annual computer security awareness training since 1992.

Criteria: Mandatory periodic training in computer security awareness and accepted computer security practices is required by 40 U.S.C. § 759 for employees who are involved in managing, using, or operating each Federal computer system within or under the supervision of that agency. In addition, the Department of the Interior's "Automated Information Systems Security Handbook" requires that computer security training be provided on an ongoing basis and that refresher training be provided at least annually.

Cause: OMM information technology officials had not established policies and procedures to ensure that annual computer security awareness training was completed in accordance with applicable computer security guidelines.

Effect: Without annual training in computer security awareness and accepted computer security practices of employees who are involved in managing, using, or operating sensitive OMM computer systems, including TIMS, there is an increased risk of unauthorized disclosure of sensitive and propriety data.

Recommendations

We recommend that the Director of MMS:

1. Implement policies and procedures to ensure that OMM employees and contractor personnel who are involved with sensitive component systems receive annual computer security awareness training.

2. Ensure that training is documented in the employee human resource files.

CONTINGENCY PLANNING, BACKUP, AND DISASTER RECOVERY

C. Service Continuity

Condition: OMM did not have an effective means of recovering or continuing critical TIMS functions and operations in the event of a system failure or a disaster. Specifically, we found that:

- The Gulf of Mexico Region's April 1996 Continuity of Operations Plan had not been tested to ensure that the planned procedures for recovering TIMS and other business functions were feasible.

- Although Gulf of Mexico regional management had developed a draft plan, dated September 1999, neither the draft plan nor the April 1996 plan included recovering critical TIMS development and maintenance functions of OMM's Information Technology Division.

- Regional personnel responsible for continuing critical functions in the event of a disaster or an emergency were not trained in their roles and responsibilities described in the Continuity of Operations Plan.

- A copy of the Plan was not available at the designated off-site storage facility.

- Neither regional nor Information Technology Division personnel ensured that backup tapes of critical TIMS data and applications were routinely transferred to the off-site storage facility.

Criteria: Appendix III of Circular A-130 requires agencies to establish controls to safeguard all information processed, transmitted, or stored in Federal automated information systems. Further, the Circular requires agencies to establish a contingency plan and periodically test the plan for the capability to perform the agency function supported by the application in the event of failure of its automated support. In addition, NIST Special Publication 800-12, "An Introduction to Computer Security: The NIST Handbook," recognizes that the success of recovering all information systems operations and data is largely dependent upon the adequacy of contingency planning, including backup and recovery procedures and testing of the plans; requires that personnel be trained in their contingency-related duties; and requires that contingency plans be stored in a safe place. The Department of the Interior's "Automated Information Systems Security Handbook" and the MMS Manual mandate routine cyclical off-site storage for all automated information

CONTINGENCY PLANNING, BACKUP, AND DISASTER RECOVERY

systems data and applications providing critical support to the organization's mission.

Cause: OMM information technology officials did not ensure that adequate service continuity controls were in place for critical TIMS functions and operations to continue without undue interruption if unexpected events occurred, such as a system failure. In addition, OMM management did not ensure that critical and sensitive TIMS application components and data were protected by being stored off-site on a routine cyclical basis.

Effect: In the event of a disaster or a system failure, OMM was at risk of not being sufficiently prepared to recover critical TIMS functions and continue critical operations.

Recommendations

We recommend that the Director of MMS:

1. Develop a Continuity of Operations Plan for the Offshore Minerals Management Information Technology Division, which includes procedures for recovery of the Division's critical TIMS functions.

2. Periodically test the Continuity of Operations Plan and update the Plan based on the test results.

3. Ensure that copies of the Continuity of Operations Plan are maintained at the off-site facility.

4. Ensure that backup copies of TIMS applications, components, and data are stored at the off-site storage facility on a routine cyclical basis.

5. Provide training to OMM personnel who are responsible for the recovery of critical TIMS business functions and operations about their roles and responsibilities related to the Continuity of Operations Plan.

SYSTEM ACCESS CONTROLS

D. User Access

Condition: OMM did not adequately control access to TIMS databases. Specifically, employees who were no longer employed by MMS still had access to TIMS. For example, we found that 28 percent of employees who had terminated their employment still had access to the TIMS Gulf of Mexico regional production database; 6 percent of departed employees, including the prior Database Administrator, had access to the TIMS development database; and 13 percent of departed employees had access to the TIMS Customer User Acceptance Team, the testing database. In addition, 798 users had access to the Customer User Acceptance Team's database when there were only 79 team members who were authorized to access the database.

Criteria: NIST's Special Publication 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems," states:

> It is necessary to periodically review user account management on a system. Reviews should examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, [and] whether management authorizations are up-to-date.

Cause: OMM Gulf of Mexico regional and Information Technology Division officials did not ensure that controls were in place to delete employee access to TIMS when employees departed the organization.

Effect: As a result, the risk was significantly increased that unauthorized users could gain access to sensitive and mission-critical TIMS data and applications.

Recommendations

We recommend that the Director of MMS:

1. Implement controls to ensure that access to TIMS for employees who have terminated employment is removed in a timely manner.

2. Ensure that access to the Customer User Acceptance Team database is limited to authorized users.

SYSTEM ACCESS CONTROLS

E. Number of Log-In Attempts

Condition: OMM's number of unsuccessful log-in attempts to access TIMS exceeded the standard established by the Department of the Interior. Specifically, TIMS users were allowed six unsuccessful log-in attempts before the user was locked out of the system.

Criteria: The Department's "Automated Information Systems Security Handbook" specifies three as the number of unsuccessful log-in attempts.

Cause: OMM information technology officials did not ensure that the number of allowed unsuccessful log-in attempts was established in accordance with Departmental standards. OMM information officials stated that log-in attempt policies were set using the default settings recommended by the software vendor and the defaults set by the Royalty Management Program. However, security management officials of the Royalty Management Program had requested and were granted a waiver to deviate from the Departmental standard by the Department's Office of Information Resources Management.

Effect: As a result, the increased number of invalid attempts reduced the effectiveness of the password as an access control. In addition, the risk was increased for unauthorized access to sensitive TIMS data.

Recommendation

We recommend that the Director of MMS evaluate the risk involved in deviating from the Department of the Interior standard for the number of unsuccessful log-in attempts. If the Director determines that the number of invalid attempts should remain at six, OMM management should request a waiver from the Department to deviate from the standard of three attempts.

SYSTEM ACCESS CONTROLS

F. Password Management

Condition: The password controls established by OMM in the Windows NT operating system allowed all system users to retain passwords indefinitely, even though the system required users to change their passwords after 90 days. The controls did not require that a password history be maintained, and the controls allowed users to change their passwords consecutively until the original password could be reused.

Criteria: The security of a password system is dependent upon keeping passwords secret. NIST Federal Information Processing Standards Publication 112, "Password Usage," states that passwords "should be changed periodically with a maximum interval selected by the Security Officer." The Publication further states that the system "should check that the new password is not the same as the previous password" or any number of previous passwords and maintain a history of the passwords of each user.

Cause: OMM information technology officials did not change Windows NT password default settings to ensure that passwords were not reused or cycled through quickly.

Effect: As a result, the risk was increased that a password could be discovered and used to obtain improper access to TIMS.

Recommendation

We recommend that the Director of MMS implement controls to ensure that system software settings are established to prevent users from reusing passwords or cycling through passwords quickly.

SOFTWARE DEVELOPMENT AND CHANGE MANAGEMENT

G. Software Change Request and Approval Process

Condition: At the Gulf of Mexico Region, formal software change control procedures had been developed and implemented for the ongoing support and maintenance of TIMS. However, we found that OMM Information Technology Division personnel did not ensure that change requests were received from authorized users; that the changes were coordinated among all the OMM regions; and that all changes were reviewed, approved, and prioritized by the OMM Maintenance Change Board. During October 1998 through June 1999, there were 1,157 change requests for TIMS, of which we statistically selected 132 changes[1] to determine the adequacy of the change management process. We found that of the 132 sampled change requests, 24 change requests (19 percent) were not submitted by an authorized user representative and 130 change requests (98 percent) were not coordinated with user representatives in the other three OMM regions. We also found no documentation to support that the changes had been reviewed and prioritized by the Maintenance Change Board.

Criteria: NIST Federal Information Processing Standards Publication 106, "Guideline on Software Maintenance," prescribes guidelines for maintaining software. According to the Publication, the primary purpose of change control (or change management) is to ensure smooth operational continuity and orderly evolution of the system. Effective change controls are needed to ensure that all software installations are performed in a structured and controlled manner and provide management with a chronological history of all software modifications. Key change management control points ensure that all changes to hardware and software are formally requested, approved, and documented. In addition, the Publication states that "there should be a centralized approval point for all software maintenance projects." Also, the "TIMS Methodology Handbook" states that Customer User Acceptance Team "leaders in the regions [should] coordinate program changes and issues among themselves before submitting a written request to the Information Technology Division." In addition, the Handbook requires the Maintenance Change Board to review and prioritize software change requests.

Cause: Division personnel did not enforce OMM policies and procedures that required change requests to be accepted from Customer User Acceptance

[1] Although we selected 132 change requests for review, we did not review all of the requests for specific attributes because some of the requests selected were canceled or were not completed at the time of our review.

SOFTWARE DEVELOPMENT AND CHANGE MANAGEMENT

Team leaders only, to be coordinated among the OMM regions, and to be reviewed and prioritized.

Effect: As a result, the risk is increased that operational problems will be introduced into the TIMS production environment. Because change requests result in changes to the TIMS production environment and implemented in all OMM regions, the lack of controlling and coordinating change requests among the Customer User Acceptance Team leaders could result in changes being made for one region that affect another region's ability to access and process transactions efficiently and effectively. Further, the resultant errors and production problems could be time-consuming and difficult to diagnose and correct. Additionally, without reviews and prioritization of change requests, there is little assurance that the most critical changes will be implemented first.

Recommendations

We recommend that the Director of MMS:

1. Enforce TIMS change control policies and procedures to ensure that all modifications are properly coordinated, authorized, approved, reviewed, and prioritized.

2. Evaluate the current policy for submitting changes to TIMS and determine whether the number of authorized persons who submit software changes can be reduced.

SOFTWARE DEVELOPMENT AND CHANGE MANAGEMENT

H. Testing

Condition: Testing and documentation of software changes to TIMS were not adequate. Specifically, we found that, of the108 changes tested, 62 changes (57 percent) did not have test plans. In addition, 24 (24 percent) of 100 changes were not tested by either the quality assurance group or the user group (see footnote 1 in Finding G).

Criteria: Publication 106 states that testing standards and procedures "should define the degree and depth of testing to be performed and the disposition of test materials upon successful completion of the testing." Also, the Publication states that testing is a critical component of software maintenance and that test plans should define the expected output of a test and test for valid, invalid, expected, and unexpected cases. In addition, the "TIMS Methodology Handbook" states that test plans are to be developed and kept current for each of the TIMS components. Test plans also became required documentation in 1998.

Cause: Although OMM had policies and procedures for software development and change management, OMM management did not ensure that the software change policies and procedures were complied with.

Effect: As a result, the risk was increased that processing irregularities or malicious codes could be introduced, sensitive data could lack integrity, and TIMS applications may not function to meet user requirements.

Recommendation

We recommend that the Director of MMS enforce its policies and procedures for developing test plans, testing software changes, and documenting test results for all changes made to TIMS.

APPENDIX 2

COMPONENTS OF TECHNICAL INFORMATION MANAGEMENT SYSTEM

Adjudication Tracking System (ATS)
Block and Boundary
Supplemental Bonding
Certs
Civil Penalty
Company and Bonding
Element Data Dictionary
Environmental: Coris
Environmental: Physical
Environmental: Social
Events
Form Navigation
Geologic
Inspections
Lease Administration
Lease Status
Lease Suspensions
Meters
Oil Spill Financial Responsibility
Performance review
Pipelines
Plans
Platforms
Post Sale
Presale
Production
Public Information
Rate Control
Reserves
Rigs
Royalty Relief
Sale
Sampling
Security
Seismic
TIMS Methodology
TIMS Shared
TIMS Support library
Tract Evaluation
Units
Wells

United States Department of the Interior

MINERALS MANAGEMENT SERVICE
Washington, DC 20240

JUL 19 2000

Memorandum

To: Assistant Inspector General for Audits

Through: for Sylvia V. Baca Piet deWitt JUL 24 2000
Assistant Secretary, Land and Minerals Management

From: Walt Rosenbusch Thomas R Kitsos, for
Director, Minerals Management Service

Subject: Office of Inspector General Draft Audit Report, "General and Application Controls Over the Technical Information Management System, Offshore Minerals Management, Minerals Management Service" [A-IN-MMS-001-99-R]

Thank you for the opportunity to respond to the draft audit report on our Technical Information Management System. We are providing to you our general comments on the audit findings and specific ones on the recommendations. We agree with all 15 recommendations and are in the process of implementing them.

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

Attachment

Minerals Management Service Response to Draft Audit Report
"General and Application Controls System"

Audit Agency: Office of Inspector General

Report Number: A-IN-MMS-001-99-R (May 2000)

GENERAL COMMENTS

We appreciate the opportunity to review and comment on the Office of Inspector General's draft audit report referenced here. Overall, we believe this was a fair evaluation of the Technical Information Management System in our New Orleans Office. We concur with all the recommendations provided in the report. We will respond to each of the eight weaknesses identified by providing (1) how we have already addressed improving the controls over TIMS, (2) how we plan to address improving the controls that are not currently in place, or (3) information in support of the controls we have in place, and therefore challenge the findings of the OIG.

COMMENTS ON WEAKNESSES AND RECOMMENDATIONS

A. **Computer Security Plan:** MMS had not developed a security plan for TIMS, which has been identified by MMS as a sensitive and mission critical system.

Recommendation A1. We recommend that the Director of MMS ensure that a computer security plan for TIMS is developed, implemented, and monitored in accordance with the United States Code, Office of Management and Budget Circular A-130, and National Institute of Standards and Technology guidelines.

Response: AGREE – MMS has identified TIMS as a sensitive and mission critical system. Because of this designation, the Offshore Minerals Management Program had a draft security plan that was provided to the OIG Auditor. This plan was in addition to the TIMS Y2K document addressed in the Report. We agree that our plan did not meet the statutory requirements for a security plan. During the audit, OMM began the development of a plan to meet the requirements addressed in OMB Circular A-130, Appendix III, and NIST Special Publication 800-18.

The responsible official is the Chief, Information Technology Division

Target Date: We plan to have a draft document prepared for review by the end of October 2000 and a final computer security plan completed by no later than **March 2001.** By the time the security plan for TIMS is completed, all OMM users will have been trained on their security responsibilities in the use of the system.

B. **Computer Security Training:** Mandatory computer security awareness training had not been provided to OMM employees and contractor personnel.

Recommendation B1. Implement policies and procedures to ensure that OMM employees and contractor personnel who are involved with sensitive component systems receive annual computer security awareness training.

Response: AGREE - OMM has not held periodic training as required by the Computer Security Act of 1987 (P.L.100-235) for "all employees [and contractors] who are involved with the management, use, or operation of each Federal computer system within or under the supervision of that agency." We are in the process of developing and implementing policies and procedures to ensure that employees and contractor personnel receive periodic computer security awareness training. Nowhere in the laws and regulations did we find that the training is mandatory on an annual basis. OMM will provide security awareness training for new employees and contractors within 60 days of working on the OMM systems. All new employees and contractors must complete a Computer Services Access Request form prior to receiving an account on the MMS computer system. This request form includes five security statements that require the user's signature before the account is assigned.

OMM has appointed a new security officer and recently hired a security specialist to develop, implement, and monitor security policy. These individuals also are charged with the development and implementation of a computer security awareness training program for users, systems administrators, and management within OMM. All OMM employees and contractors will participate in a security awareness-training program before the end of Calendar Year 2000. All employees will have, at a minimum, computer awareness training every even numbered calendar year. Periodic security alerts will be sent to all employees on an as needed basis, or as conditions warrant an update.

Recommendation B2. Ensure that training is documented in the employee human resources files.

Response: AGREE - OMM will ensure that the computer security awareness training is documented in the employee's human resources file.

The responsible official is the Deputy Associate Director for Offshore Minerals Management.

Target date: We will train all OMM employees and contractors in computer security awareness by **December 2000.**

C. **Service Continuity:** OMM did not have an effective means of recovering or continuing critical TIMS functions and operations in the event of a system failure or a disaster. The Gulf of Mexico Region's April 1996 Continuity of Operations Plan has not been tested. The Plan did not include recovering critical TIMS development and maintenance functions. The Regional personnel responsible for the Plan had not been trained in their roles and responsibilities. The Plan was not available at the designated offsite storage facility. The backup tapes of critical TIMS data and applications were not routinely transferred to the off-site storage facility.

Recommendation C1. Develop a Continuity of Operations Plan for the Offshore Minerals Management Information Technology Division, which includes procedures for recovery of the Division's critical TIMS functions.

Response: AGREE – Since the audit was conducted, OMM has reorganized various functions within the New Orleans Office. We have moved all TIMS server hardware, development, and Gulf of Mexico Region production under one management structure. A new Continuity of Operations Plan has been finalized for the New Orleans computer center that includes all hardware operations at that location. The Plan also includes procedures for the recovery of critical TIMS functions.

Recommendation C2. Periodically test the Continuity of Operations Plan and update the Plan based on the test results.

Response: AGREE – We plan to test the New Orleans Continuity of Operations Plan prior to the end of Calendar Year 2000 and on a regular basis in the future.

Recommendation C3. Ensure that copies of the Continuity of Operations Plan are maintained at the offsite facility.

Response: AGREE – An updated copy of the Continuity of Operations Plan can be found in the Headquarters office of the Information Technology Division and also at a new offsite storage facility in the New Orleans area.

Recommendation C4. Ensure that backup copies of TIMS applications, components, and data are stored at the offsite storage facility on a routine cyclical basis.

Response: AGREE – We have established and implemented new backup procedures. We also store backup copies of the TIMS applications, components, and data at the new offsite storage facility in the New Orleans area. These items are rotated on a routine basis as defined in the Continuity of Operations Plan. All boxes are clearly labeled for quick recovery.

Recommendation C5. Provide training to OMM personnel who are responsible for the recovery of critical TIMS business functions and operations about their roles and responsibilities related to the Continuity of Operations Plan.

Response: AGREE – We will train OMM personnel concerning their roles and responsibilities for the recovery of critical TIMS business functions and operations.

The responsible official is the Regional Director, Gulf of Mexico Region.

Target date: Test New Orleans Continuity of Operations Plan by **December 2000.**

D. User Access: OMM did not adequately control access to the TIMS databases. Specifically, employees who were no longer employed by MMS still had access to the TIMS.

Recommendation D1. Implement controls to ensure that access to TIMS for employees who have terminated employment is removed in a timely manner.

Response: <u>AGREE</u> –When an employee leaves the Bureau, a procedure is in place to terminate all access to the MMS and TIMS systems.

Recommendation D2. Ensure that access to the Customer User Acceptance Team database is limited to authorized users.

Response: <u>AGREE</u>: - We have implemented new procedures to ensure that access is available only to those who have a need to know the TIMS information. Procedures have also been put in place to provide access to only those who have completed a user access form. The Office of Responsibility must also grant permission prior to the user having access to the TIMS data. We have established a database to track user access to the TIMS system. The same procedures will be followed for all employees requiring access to the Customer User Acceptance Team database.

The responsible official is the Deputy Associate Director, Offshore Minerals Management.

Target date: Task Completed.

E. **Number of Log-In Attempts:** OMM's number of unsuccessful log-in attempts to access TIMS exceeded the standard established by the Department of the Interior. Specifically, TIMS users were allowed six unsuccessful log-in attempts before the user was locked out of the system.

Recommendation E1. MMS should evaluate the risk involved in deviating from the Department of the Interior standard for the number of unsuccessful log-in attempts. If the Director determines that the number of invalid attempts should remain at six, OMM management should request a waiver from the Department to deviate from the standard of three attempts.

Response: <u>AGREE</u> – The number of unsuccessful log-in attempts has been established at three unsuccessful log-in attempts before the user is locked out of the system.

The responsible official is the Deputy Associate Director, Offshore Minerals Management.

Target Date: Task Completed.

F. **Password Management:** The password controls established by OMM in the Windows NT operating system allows all system users to retain passwords indefinitely, even though the system required users to change their passwords after 90 days. The controls did not require that a password history be maintained, and the controls allowed users to change their passwords consecutively until the original password could be reused.

Recommendation F1. MMS should implement controls to ensure that system software settings are established to prevent users from reusing passwords or cycling through passwords quickly.

Response: AGREE - All NT servers that are supported by OMM and MMS have the password setting to prevent the reuse or quick recycling of passwords. These passwords must be changed every 90 days. The Council of Information Management Officials established this policy on behalf of the Bureau.

The responsible officials are members of the Council of Information Management Officials.

Target Date: Task Completed.

G. **Software Change Request and Approval Process:** At the Gulf of Mexico Region, formal software change control procedures had been developed and implemented for the ongoing support and maintenance of TIMS. However, we found that OMM Information Technology Division personnel did not ensure that change requests were received from authorized users; that the changes were coordinated among all the OMM regions; and that all changes were reviewed, approved, and prioritized by the OMM Maintenance Change Board. We also found no documentation to support that the changes had been reviewed and prioritized by the Maintenance Change Board.

Recommendation G1. Enforce TIMS change control policies and procedures to ensure that all modifications are properly coordinated, authorized, approved, reviewed, and prioritized.

Response: AGREE: - The Information Technology Division has not been in the position to reject the TIMS maintenance and/or enhancement change requests submitted by the program office. In the early development of TIMS, OMM established the Component User Acceptance Team leader concept for each major subject area of TIMS to be the focal point for ongoing program changes. The Teams are responsible for the program view and coordination of their respective components. The Information Technology Division implemented the change requests as submitted.

To deal with the large number of change requests, the TIMS Project Office established a Change Control Group (called Maintenance Change Board in the Report). The Information Technology analyst who knew the design and was responsible for the maintenance of the TIMS components was a member of this Group. The TIMS Maintenance Methodology states that all requests will be reviewed and prioritized, and deadlines will be set for implementation. All change requests are entered into the tracking system called Defect Control System. The Change Control Group reviewed all outstanding work requests in the Defect Control System and made assignments to the staff, weekly. The tracking of the request in the Defect Control System was the documentation.

The OMM Information Technology Division staff did not track nor collect information in reference to the Component User Acceptance Team coordinating change requests with peers in other regions. That is the responsibility of the Team leader. Upon completion of a work request of the Information Technology Division staff, all Component User Acceptance Teams for that component were notified by the Information Technology Division that the work request was completed. The module was then ready for testing prior to final deployment to all OMM sites.

In October 1999, the Information Management Committee determined that it needed to better manage the change control policies and procedures. The Committee authorized the creation of a new TIMS Change Control Board. The Board is comprised of representatives from the OMM program offices and Chaired by the Deputy Regional Director of the Gulf of Mexico Region. The purpose of the Change Control Board is to review, monitor, evaluate, approve/ disapprove, and prioritize all enhancement and maintenance requests (submitted by the TIMS users) for current TIMS components. The Board will also review usage of the TIMS forms and reports and eliminate unused or underutilized and non-critical forms and reports.

With the development of this Board, all programmatic changes, corrections, amendments, reforms, improvements, enhancements, or upgrades made to the TIMS components are reviewed, approved/disapproved, and prioritized. This review also entails an evaluation of the potential costs and benefits of proposed changes.

Recommendation G2. Evaluate the current policy for submitting changes to TIMS and determine whether the number of authorized persons who submit software changes can be reduced.

Response: AGREE - The Change Control Board is not only responsible for enforcing the change control policies and procedures, but also controls the number of changes that can be made to the system. The Information Technology Division is in the final stage of implementing a replacement for the work request tracking system known as Defect Control System. The new software system is a commercial off-the-shelf solution called Visual Interceptor. Interceptor is web based and will only allow authorized Component User Acceptance Teams to forward approved work requests to the Change Control Board for final review and prioritization. This new web-based system will be in place by the end of calendar year 2000.

The responsible official is the Deputy Associate Director for Offshore Minerals Management.

Target Date: Policy to limit number of persons submitting changes – Completed.
Implementation of request tracking by **December 2000.**

H. **Testing:** Testing and documentation of software changes to TIMS were not adequate. Specifically, we found that, of the 108 changes tested, 62 changes (57 percent) did not have test plans. In addition, either the quality assurance group or the user group did not test 24 of 100 (24 percent) changes.

Recommendation H1. MMS should enforce its policies and procedures for developing test plans, testing software changes, and documenting test results for all changes made to TIMS.

Response: AGREE – We agree with the recommendation made in the report that OMM should enforce the TIMS Maintenance Methodology policies and procedures related to testing and its documentation. We **do not agree** with the analysis that drew the auditors to their recommendations. Based on our analysis of the full 132 sample set, our findings are different from the auditor. Specifically, of the 62 changes (57 percent) that did not have individual test plans, OMM determined 59 changes to be exceptions that did not require test plans. Although the TIMS Maintenance Methodology requires test plans, there are certain changes that are considered routine and/or minor and, therefore, would not require individual test plans. These exceptions include reports (41); and system administration functions, database triggers, packages, and menu change requests (18). Therefore, OMM found that only 3 of the 62 changes should have had test plans based on the TIMS Maintenance Methodology. Reports are covered by a generic test plan since they are fairly simple and do not require individual test plans.

In addition, we concur that the quality assurance or the user group did not test 24 of 100 changes. We determined that there were 20 exceptions to these changes. These exceptions included data dictionary, domain value, or menu changes. The Database Administrator makes these changes and, upon completion, the Component User Acceptance Team members or an analyst tests the change. We conclude that there were only four changes that were not tested before they were put on the production machine. Therefore, the quality assurance group or the user group did not test only 4 percent of the changes.

The Information Technology Division is converting to a new change control tracking system, called Visual Interceptor, that will better serve our customers with online web access to the status of all change requests. We will properly identify all stages of the life cycle of a change request. This new system should be fully operational by the end of the calendar year 2000. A change request can be submitted for many Information Technology functions, not just a change to a TIMS program.

We recognize the need for test plans and for adequate testing of the changes, and we plan to continue this process. We also have tightened up and enforced the policies and procedures we have in place. There are numerous exceptions and alternative test procedures that accompany the change management. These exceptions need to be further identified in our TIMS Maintenance Methodology. We will continue our review of existing methodology to expand testing and acceptance criteria to improve the process. Documentation will occur through the implementation of the new change control tracking system.

The responsible official is the Deputy Associate Director for Offshore Minerals Management.

Target Date: Enforcement of required test plans and testing – Completed.
Implementation of request tracking by **December 2000.**

STATUS OF AUDIT REPORT RECOMMENDATIONS

Finding/Recommendation Reference	Status	Actions Required
A.1, B.1, B.2, C.2, C.5, G.2, and H.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.
C.1, C.3, C.4, D.1, D.2, E.1, F.1, and G.1	Implemented.	No further response is required.

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.
Mail Stop 5341 - MIB
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

HOTLINE

U.S. Department of the Interior
Office of Inspector General
1849 C Street, NW
Mail Stop 5341- MIB
Washington, D.C. 20240-0001

Toll Free Number
1-800-424-5081

Commercial Numbers
(202) 208-5300
TDD (202) 208-2420