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

AUDIT REPORT

GENERAL AND APPLICATION CONTROLS OVER AUTOMATED INFORMATION SYSTEMS, OFFICE OF SURFACE MINING RECLAMATION AND ENFORCEMENT

REPORT NO. 00-I-138
DECEMBER 1999

United States Department of the Interior

OFFICE OF INSPECTOR GENERAL
Washington, D.C. 20240

DEC 21999

AUDIT REPORT

Memorandum

To: Director, Office of Surface Mining Reclamation and Enforcement

From: Robert J. Williams
Assistant Inspector General for Audits

Subject: Audit Report on General and Application Controls Over Automated Information Systems, Office of Surface Mining Reclamation and Enforcement **(No.** 00-I-138)

INTRODUCTION

This report presents the results of our audit of the Office of Surface Mining Reclamation and Enforcement's general and application controls over its automated information systems. The objective of this audit was to determine whether Surface Mining had effective general and application controls over its automated information systems and whether the automated information systems were operating in compliance with the Federal Financial Management Improvement Act. We performed this audit to support the Office of Inspector General's opinion on the financial statements of Surface Mining by evaluating the reliability of the general and application controls over computer-generated data that support Surface Mining's annual financial statements.

BACKGROUND

The Office of Surface Mining Reclamation and Enforcement was created with the enactment of the Surface Mining Control and Reclamation Act of 1977 (Public Law 95-87). The purpose of Surface Mining is to implement the provisions of the Surface Mining Control and Reclamation Act and to ensure that society and the environment are protected from the adverse effects of surface and subsurface coal mining operations. Surface Mining meets this mission through programs authorized by Title IV (Abandoned Mine Reclamation) and Title V (Control of the Surface Effects of Coal Mining) of the Surface Mining Control and Reclamation Act. Surface Mining's activities include issuing mine permits, inspecting mine operations, enforcing mine standards, ensuring the effectiveness ofauthorized state and tribal regulatory programs, and promoting reclamation of surface mine lands.

Surface Mining has its headquarters in Washington, D.C., and has decentralized its regulatory and enforcement mission through the Appalachian Regional Coordinating Center, in Pittsburgh, Pennsylvania; the Mid-Continent Regional Coordinating Center, in Alton, Illinois; and the Western Regional Coordinating Center, in Denver, Colorado. Additionally, Surface Mining maintains a close working relationship with governments of the coal-producing states, environmental protection groups, and mission support contractors.

Surface Mining is dependent on automated information systems to support its mission and financial statements. The Division of Information Systems Management is responsible for facilitating the efficient and effective use of information and information technologies in support of information resources management and Surface Mining's mission. The information resources management responsibilities are shared by various Surface Mining organizations, including the Division of Information Systems Management, the Division of Financial Management, assistant directorates, and regional and field offices. Nationwide, automated data processing support is provided through local area network-based microcomputer workstations, including Windows NT, Silicon Graphics, and Sun Solar-is UNIX. The local area networks are interconnected by Surface Mining's wide area network.

The data center responsible for inputting, recording, classifying, and reporting on Surface Mining's financial business is located at the Division of Financial Management in Denver. The Division operates and maintains two minicomputer platforms, a Hewlett Packard and a Sun Solaris, to support Surface Mining's financial management functions. The Hewlett Packard computer hosts Surface Mining's primary financial management system, the Advanced Budget/Accounting Control and Information System (ABACIS). In addition, the Hewlett Packard computer hosts other financial applications that affect the generation of financial statement information as follows:

- The Grants Information Fund Tracking System (GIFTS)
- The Civil Penalty Accounting Control System (CPACS)
- The Audit Fee Billing and Collection System (AFBACS)
- The Synergistic Acquisition Tracking and Information Network (SATIN)

The Sun Solaris computer hosts the Fee Billing and Collection System (FEEBACS) application, which generates records for posting to ABACIS and affects the generation of financial statement information. In addition, FEEBACS supports Surface Mining's mission critical Applicant Violator System (AVS), which is an independent, stand-alone system that does not generate data for or impact Surface Mining's financial records and statements. Also, the Division operates a Windows NT computer network that distributes personnel data to Surface Mining's human resource and budget personnel and provides financial management data to Surface Mining's users.

Systems security policies for Surface Mining are established by its Information Technology Security Officer. System security administration for the minicomputers, local area networks, and the wide area network is the responsibility of the information technology security officers at Surface Mining offices and facilities.

SCOPE OF AUDIT

We reviewed Surface Mining's general controls (the policies and procedures for ensuring that information systems operate properly) that were in place for its automated information systems. We did not review the application controls (the controls over input, processing, and output of data) because of the weaknesses we found in the general controls. The effectiveness of the general controls determines the effectiveness of the application controls. When the general controls are not effective, application controls can be made ineffective because the application controls can be bypassed or modified.

We reviewed the general controls in six major areas: security program development, logical and physical access, change management, separation of duties, system software, and service continuity. To accomplish our objective, we interviewed Surface Mining and contractor personnel, reviewed systems documentation, observed and became familiar with data center operations and network components, analyzed systems security, and evaluated service continuity procedures and testing. In addition, we reviewed the software maintenance procedures. During the audit, we used several software tools to identify vulnerabilities in Surface Mining's automated information systems and networks. These tools were used to perform a variety of functions, such as monitoring and analyzing user and system activity, auditing system configurations and vulnerabilities, accessing the integrity ofcritical systems and data files, and operating system audit-trail management. Because our review was limited to evaluating the adequacy of general controls over automated information systems, we did not evaluate the effectiveness of manual control procedures that may have operated as compensating controls for the automated information systems' general controls.

Our audit, which was conducted during January through April 1999 at Surface Mining's headquarters and the data center in Denver, Colorado, 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 evaluated the internal controls that could adversely affect Surface Mining's automated information systems. The control weaknesses that we found are summarized in the Results of Audit section and detailed in Appendix 1 of this report. Based on our determination of the inadequacy of the general controls taken as a whole, we believe that the weaknesses in Surface Mining's general controls over its automated information systems should be reported as a "reportable condition" in Surface Mining's annual financial statements for fiscal year 1999. In addition, Surface Mining did not have security plans for its 13 sensitive systems. We believe that Surface Mining should report the lack of security plans for the systems as a material weakness in its annual assurance statements on management controls for fiscal year 1999. 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.

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 the Office of Surface Mining Reclamation and Enforcement's general controls over its automated information systems.

RESULTS OF AUDIT

We concluded that the Office of Surface Mining Reclamation and Enforcement's general controls over its automated information systems were not effective. Specifically, Surface Mining did not have an adequate security program; did not have controls over access to automated information systems resources, systems software, separation of duties, and software development and change management; and did not have assurance of continued operations in the event of a disaster or system failure. Office of Management and Budget Circular A- 130, "Management of Federal Information Resources," 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 information in the computer systems of executive branch agencies. Additionally, the Congress enacted laws, such as the Privacy Act of 1974 and the Computer Security Act of 1987, 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. The Computer Security Act defines "sensitive" data 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 the Privacy Act." Further, the Department of the Interior and Surface Mining have issued policies and procedures to implement general controls to protect sensitive data in automated information systems. However, the general controls were not adequate because Surface Mining management had not (1) established necessarypolicies and procedures for the controls, (2) assigned responsibilities for ensuring that policies and procedures were developed and followed, and (3) held officials accountable for noncompliance with the established controls. The lack of adequate controls increased the risk of unauthorized access and modifications to and the disclosure of Surface Mining data, theft or destruction of Surface Mining software and sensitive information, and loss of critical Surface Mining systems and functions in the event of a disaster or system failure.

Overall, we identified 16 weaknesses and made 38 recommendations for improving the general controls over Surface Mining's automated information systems. A summary of the weaknesses noted in the six major areas reviewed is provided in the paragraphs that follow, and specific details of the weaknesses and our respective recommendations to correct these weaknesses are in Appendix 1.

Security Program

We found that Surface Mining did not have an automated information systems security program which identified and addressed all risks affecting sensitive and financial data, did not have security plans for its 12 sensitive automated information systems, and did not have adequate security-related personnel policies and procedures for Surface Mining employees and contractors. As a result, there was an increased risk that sensitive data may be impaired or compromised by individuals and that data may be inadvertently disclosed, destroyed, or erroneously modified. We made nine recommendations to address these weaknesses.

Access Controls

We found that Surface Mining did not have adequate controls over access to its automated information systems. Specifically, Surface Mining did not classify its automated information systems resources to determine the level of security that should be provided, control the levels of access granted to systems users, limit the number of log-in attempts allowed for access to computer resources as required by Department of the Interior standards, control passwords and password settings, control public user access to the Novell network and file servers, and protect its local area networks. As a result, there was an increased risk that sensitive data maintained on the automated information systems were vulnerable to unauthorized access, manipulation, and disclosure. We made 14 recommendations to address these weaknesses.

System Software Controls

We found that the controls over system software did not detect and determine inappropriate use and address vulnerabilities in the operating systems. Specifically, available computer systems audit tools to ensure integrity over systems processing and data were not used, some systems audit trails were not implemented and when implemented were not reviewed, and vendor updates to operating systems software were not implemented. As a result, there was an increased risk that inappropriate systems settings and processing would not be identified and recorded. Also, without periodic reviews of the systems' audit trails, there was an increased risk that processing problems or unauthorized activities may not be detected or detected in a timely manner. Additionally, there was an increased risk that operating systems' vulnerabilities addressed by the vendor would not be corrected. We made six recommendations to address these weaknesses.

Separation of Duties

We found that Surface Mining management did not separate the duties of system security administrators from reviewers and did not separate the duties of the application programmers from systems users. As a result, there was an increased risk that inappropriate actions by security administrators would not be detected or detected timely and that accidental or intentional actions by programmers could threaten the integrity of Surface Mining's data and disrupt systems processing. We made two recommendations to address these weaknesses.

Software Development and Change Management

We found that Surface Mining did not ensure that changes to applications software were authorized, approved, and tested before being moved into production. As a result, there was an increased risk that critical sensitive applications software changes were not made and that applications would not perform as intended. We made three recommendations to address these weaknesses.

Service Continuity

We found that Surface Mining did not develop a continuity of operations plan for its telecommunications links, did not finalize plans for its facilities and data center, and did not have an incident response plan or team. As a result, there was an increased risk that critical systems or data may not be recovered in the event of a disaster or system failure. We made four recommendations to address these weaknesses.

Other Matters

During our audit, we also found that the environmental controls at Surface Mining's Information Systems Management computer operations room were not adequate to safeguard the computer resources. For example, the air conditioning system was not maintaining an appropriate room temperature; the carpeting was dirty and worn, which produces dust and debris; and the overall condition of the room was unkempt. The National Institute of Standards and Technology's "An Introduction to Computer Security: The NIST Handbook" states that computer resources, such as hardware, software, and magnetic media, require environmental protection to ensure that the computer resources are safeguarded from excessive temperatures, dust, and debris.

Office of Surface Mining Reclamation and Enforcement Response and Office of Inspector General Reply

In the September 17, 1999, response (Appendix 3) to the draft report from the Director, Office of Surface Mining Reclamation and Enforcement, Surface Mining concurred with the 38 recommendations. Based on the response, we consider Recommendations K.2, M. 1, M.2, N.2, O.2, O.3, and P. 1 resolved and implemented and Recommendation K. 1 resolved but not implemented. Accordingly, Recommendation K.l will be forwarded to the Assistant Secretary for Policy, Management and Budget for tracking of implementation (see Appendix 4). Regarding Recommendation B.3, we agree that the actions taken by Surface Mining to develop security plans for its mission critical systems are sufficient, although the plans are not complete; therefore, Surface Mining does not need to report this as a material weakness in the annual assurance statement on management controls for fiscal year 1999. Thus, we consider this recommendation resolved. Also based on the response, we request the dates and titles of the individuals responsible for implementing the remaining 30 recommendations.

Surface Mining has completed or has begun actions needed to implement the 38 recommendations. Specifically, the draft publication "Information Systems Security Program Directive" addresses many of our recommendations for developing policies and procedures to ensure that Surface Mining's automated systems are adequately safeguarded. Although Surface Mining has initiated actions to correct the general control weaknesses identified in this report, many of these actions were not completed by the end of fiscal year 1999. Therefore, we believe that the weaknesses in Surface Mining's general controls over its automated information systems should be reported as a "reportable condition" in Surface Mining's annual financial statements for fiscal year 1999.

Surface Mining's specific comments to some of the recommendations are in the paragraphs that follow.

Recommendation A.1. Surface Mining said that it had completed a risk assessment for each of its 16 mission critical systems and that these risk assessments were included in its response. However, the response did not include risk assessments for the Administrative Records Management System (ARMS); the Technical Information Processing System (TIPS); and the Work Assignment Tracking System/Mine Information, Project Planning System (WATS/MIPPS). Therefore, Surface Mining should complete risk assessments for these systems and provide target dates and titles of officials responsible for implementation.

Recommendation B.l. Surface Mining requested that we delete the Payroll/Personnel Data Entry (PAY/PERS) from our list of 13 sensitive systems because the System "is no longer used" by Surface Mining. Also, Surface Mining identified four additional systems requiring security plans. We have revised Appendix 2 to reflect these changes.

Recommendation B.2. Surface Mining said that it concurred with the recommendation; however, Surface Mining also said that it will elevate the information systems security function to report to the Deputy Chief Information Officer rather than to the Chief Information Officer (as we had recommended). We believe that this action meets the intent of the recommendation, but a target date and title of the official responsible for implementation should be provided.

Recommendation F.5. Surface Mining stated that the systems' log-in warning message cannot be the first screen displayed because of computer "hardware and operating system architecture." However, Surface Mining stated that the log-in warning message will be placed as close to the first screen as the hardware and operating system will allow. We believe that this action meets the intent of the recommendation, but a target date and title of the official responsible for implementation should be provided.

Recommendation K.3. Surface Mining said that the minicomputer platforms used by the Division of Financial Management maintain system logs and that the logs are retained for 6 months. Surface Mining also said that the audit function on the Windows NT and the Novell servers has been "enabled." However, Surface Mining needs to implement policies and procedures to ensure that the system logs are used and that the logs are controlled by

request that Surface Mining provide an action plan that includes a target date and title of the official responsible for implementing the policies and procedures.

In accordance with the Departmental Manual (360 DM 5.3), we are requesting a written response to this report by January 24, 2000. The response should provide the information requested in Appendix 4.

Section 5(a) of the Inspector General Act (Public Law 95-452, as amended) 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 copies of audit reports to the Congress.

We appreciate the assistance of Surface Mining personnel in the conduct of our audit.

DETAILS OF WEAKNESSES AND RECOMMENDATIONS

SECURITY PROGRAM

Control Objective: The control objective for the security program is to establish the framework for continually managing risk, developing system security policy, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls.

A. Risk Assessments

Condition: The Office of Surface Mining Reclamation and Enforcement did not implement a risk management process. Specifically, we found that:

- Risk assessments had not been made of Surface Mining's computer systems, applications, and computer resources.

- No overall determination had been made of the effectiveness of the technical controls implemented.

- No acceptance of the residual risk of not implementing a risk management process had occurred.

Criteria: Office of Management and Budget Circular A- 130, Appendix III, "Security of Federal Automated Information Resources," states that adequate security "includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls." Circular A-130 further states that, although formal risk analyses need not be performed, adequate security should be determined based on risk management. In implementing risk management, major factors such as "the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards" should be considered. Also, the National Institute of Standards and Technology's "An Introduction to Computer Security: The NIST Handbook" provides guidance on computer security risk management. The "NIST Handbook" specifically addresses the selection of safeguards to reduce risk and to accept any residual risk.

Cause: Surface Mining had not developed policies and procedures to establish a risk-based approach to assessing the risks to its automated information systems and taking actions to manage these risks. In addition, no one was formally assigned responsibility for conducting risk assessments; thus, risks to the automated information systems had not been identified and managed.

SECURITY PROGRAM

Effect: Without identifying all significant threats and vulnerabilities to the automated information systems, computer resources, and facilities, Surface Mining's management was unable to determine the most effective measures needed to protect against threats or reduce the vulnerabilities. Therefore, there was a risk that critical Surface Mining resources would not be adequately protected and that expensive controls would be implemented for resources which did not require significant protection.

Recommendations:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement:

1. Determine the risks associated with each of the systems and, based on the results of the risk assessments, establish appropriate security policies and procedures.

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

3. Formally assign and communicate responsibility to those individuals required to participate in assessing risks.

SECURITY PROGRAM

B. System Security Plans

Condition: Security plans for Surface Mining's 13 sensitive automated information systems (the systems are listed in Appendix 2) as reported to the Department of the Interior in Surface Mining's "Automated Information Systems Security Plan," dated February 1998, had not been developed. Also, Surface Mining had not reported the lack of security plans for the systems as a material weakness in its annual assurance statement on management controls for fiscal year 1999, as required by Office of Management and Budget Circular A-130, Appendix III.

Criteria: The Computer Security Act of 1987 requires the development of a security plan for each Federal computer system that contains sensitive information. 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 systems' integrity, availability, and confidentiality. In addition, Office of Management and Budget Circular A- 130, Appendix III, states that agencies without adequate security plans should consider classifying the lack of security plans as a material weakness in the agency's annual Federal Managers' Financial Integrity Act report to the Congress. Also, the National Institute of Standards and Technology's Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems," states that "[a]ll Federal systems have some level of sensitivity and require protection as part of good management practice" and that the method of protection must be documented in a system security plan.

Cause: Surface Mining management, rather than developing security plans for its 13 sensitive systems, said that it believed the Management Control Reviews and Alternative Management Control Reviews were sufficient to meet security plan requirements. In addition, because Surface Mining's information technology security function was within the Division of Information Systems Management's Automated Data Processing Support Team, the function did not have adequate independence and authority to implement and enforce an overall Surface Mining computer security program that would ensure that security plans were developed for Surface Mining's general support systems and major applications. We believe that, at a minimum, the position of Information Technology Security Officer should be elevated to report directly to Surface Mining's Chief Information Officer. Further, while Surface Mining had

'General support systems are an interconnected set of information resources under the same direct management control which shares common functionality.

SECURITY PROGRAM

information technology security officers at other locations, most of their time was spent in performing other duties.

Effect: Without automated information systems security plans, Surface Mining's management did not have adequate assurance that the data in its sensitive systems were adequately protected. In addition, without security plans for the 13 sensitive systems, Surface Mining had a material weakness that should be reported in its annual assurance statement on management controls for fiscal year 1999.

Recommendations:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement:

1. Provide resources to ensure that automated information systems security plans are developed for its general support systems and major applications in accordance with the Computer Security Act; Office of Management and Budget Circular A-130, Appendix III; and the National Institute of Standards and Technology's Special Publication 800-l 8.

2. Ensure that the automated information systems security function is elevated organizationally to report directly to Surface Mining's Chief Information Officer and formally provide the position with the authority to implement and enforce a computer security program throughout Surface Mining.

3. Report the lack of security plans for Surface Mining's sensitive systems as a material weakness in Surface Mining's annual assurance statement on management controls for fiscal year 1999.

SECURITY PROGRAM

C. Security-Related Personnel Policies and Procedures

Condition: Surface Mining's security-related personnel policies and procedures did not ensure systems integrity. Specifically, we found that:

- Surface Mining personnel in public trust positions, such as computer security officers, system and application programmers, and sensitive automated information system owners and managers, did not have documented background investigations for security clearances or did not have adequate position sensitivity levels commensurate with their positjons. Also, Surface Mining personnel did not have documentation to support that required periodic followup background checks had been performed.

- Critical automated data processing contractor personnel, such as system administrators and software management personnel, at the Division of Information Systems Management did not have documented background checks and security clearances.

Criteria: Office of Management and Budget Circular A-130, Appendix III, requires agencies to establish and manage personnel security policies, standards, and procedures that include requirements for screening individuals who (1) participate in the design, development, operation, or maintenance of sensitive applications or (2) have access to sensitive data. Also, the Code of Federal Regulations (5 CFR 73 1.302) requires suitability reinvestigations every 5 years for personnel filling high risk positions. Additionally, the Department of the Interior Manual (441 DM 3) specifies that public trust positions (all positions that do not have national security related duties) must be designated at "risk levels commensurate with the public trust responsibilities and attributes of the position as they relate to the efficiency of the Federal service."

Cause: Surface Mining did not have established policies and procedures for requiring background investigations for Federal and contractor personnel filling sensitive and critical public trust positions. In addition, Surface Mining did not include in two of the contracts we reviewed a requirement for contractor personnel to have background investigations.

Effect: Without adequate security-related personnel policies and procedures, Surface Mining increases the risk that sensitive automated information systems operations and data could be impaired or compromised by Federal or contractor personnel.

SECURITY PROGRAM

Recommendations:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement:

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

2. Ensure that all automated data processing contractor employees to have proper background clearances.

3. Ensure that periodic reinvestigations are completed every 5 years on personnel who are in public trust high risk positions.

ACCESS CONTROLS

Control Objective: The control objective for access controls is to limit or detect access to computer resources (for example, data, programs, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure.

D. Resource Classifications

Condition: Surface Mining had not classified its computer resources to determine the level of security that should be provided.

Criteria: Office of Management and Budget Circular A-130, Appendix III, directs agencies to assume that all major systems contain some sensitive information which needs to be protected but to focus extra security controls on a limited number of particularly high risk or major applications. Also, the Computer Security Act requires agencies to identify systems that process sensitive data.

Cause: Surface Mining did not have policies that provided for (1) information resources to be classified, (2) resource classification categories to be based on the need for protective controls, (3) senior-level management to review and approve resource classifications, and (4) determinations of resource classifications to be documented. Additionally, classification of the information resources could not be achieved because a risk assessment (which identifies threats, vulnerabilities, and the potential negative effects that could result from disclosing confidential data or from not protecting the integrity of data supporting critical transactions or decisions) had not been performed on the computer applications and systems software.

Effect: If information resources are not classified according to their criticality and sensitivity, there is little assurance that Surface Mining is providing the most cost-effective means to protect the computer resources.

Recommendation:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement, develop and implement policies to classify Surface Mining's computer resources in accordance with the results of periodic risk assessments and guidance contained in Office of Management and Budget Circular A-l 30, Appendix III.

ACCESS CONTROLS

E. Access Levels

Condition: Surface Mining did not have adequate controls in place to ensure that access levels granted to users of their automated information systems were appropriate. For example, we found that 14 personnel were granted "super-user" rights to the Fee Billing and Collection System (FEEBACS). Therefore, these users can manipulate FEEBACS databases, thus bypassing normal transaction processing controls.

Additionally, we found that access approval documentation was not available for all users on the systems. For example, based on a statistical sample of users selected for each of the operating and sensitive application systems reviewed, we found that access approval documentation was not available for:

- 20 (100 percent) of the users of the Novell operating system.
- 63 (80 percent) of 78 of the users of the Sun Solaris operating system.
- 3 1 (88 percent) of 35 of the users of the Windows NT operating system.
- 18 (16 percent) of 109 of the users of the financial system application.
- 20 (66 percent) of 30 of the users of FEEBACS application.

In addition, we found that access granted to users of these systems had not been approved by the system owners or managers and that periodic reviews had not been performed to determine who the users were and whether the levels of access granted in the automated information systems were appropriate. We also found that individuals whose employment had been terminated had access to the systems.

Criteria: The National Institute of Standards and Technology's "Generally Accepted Principles and Practices for Securing Information Technology Systems" states:

> Organizations should ensure effective administration of users' computer access to maintain system security, including user account management, auditing and the timely modification or removal of access. ... Organizations should have a process for (1) requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions . . . [and] it is necessary to periodically review user account management on a system. Reviews should examine the levels of access

ACCESS CONTROLS

each individual has, conformity with the concept of least privilege, whether all accounts are still active, [and] whether management authorizations are up-to-date.

The Department of the Interior Manual (375 DM 19, "Information Technology Security"), states, "Since the greatest threat to most computer systems comes from authorized users, bureaus should institute personnel controls such as least privilege, separation of duties, and individual accountability." Further, the Manual states, "Detailed procedural guidelines will be established ... to ensure IT [information technology] resources are properly protected and used only by authorized personnel."

Cause: Surface Mining management had not established policies to implement a process of approving access to its automated information systems. In addition, there was no formal assignment of responsibility for approving systems access and for periodically reviewing access levels granted to system users. Also, procedures had not been implemented to ensure that system administration personnel were promptly notified of changes in employee assignments or employment terminations.

Effect: As a result, there was a risk that unauthorized access, data manipulation, and disclosure of sensitive information may occur and that the unauthorized access would not be detected or detected timely.

Recommendations:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement:

1. Institute a policy of "least privilege" access levels to ensure that access to resources and data is limited to those users who require such access.

2. Develop and implement policies and procedures for approving access to the automated information systems that include the formal assignment of responsibility for approving systems access.

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

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

5. Implement controls to ensure that system owners approve all access to their applications in accordance with Surface Mining policy.

ACCESS CONTROLS

F. System Log-in

Condition: The number of unsuccessful log-in attempts to access Surface Mining's automated information systems exceeded the standard established by the Department. Specifically, we found that:

- Windows NT users were allowed unlimited unsuccessful log-in attempts. However, during our review, Surface Mining officials temporarily changed the setting to nine, with plans to change the setting to the standard of three attempts.

- Sun Solaris system users were allowed five unsuccessful log-in attempts before their user identifications (ID) and passwords were revoked,

- Financial system users were allowed eight unsuccessful log-in attempts before their user IDs and passwords were revoked. However, during our review, Surface Mining officials implemented new software and reduced the setting to the standard of three.

Additionally, the system log-in warning message that is used to warn potential unauthorized users that prosecution may occur was not displayed until after the user had logged on to the system and was authenticated as a valid system user.

Criteria: The Department of the Interior's "Automated Information Systems Security Handbook" states that "unsuccessful attempts to enter a password should be limited to three attempts." Further, the "Handbook" requires that all communications equipment capable of displaying system messages display, as the first message seen by a user, a warning message regarding unauthorized use of Government computers and/or software.

Cause: Although two of the three system administration personnel changed the number of log-in attempts, Surface Mining management had not developed polices and procedures that would implement the minimum standards established by the Department throughout Surface Mining. Additionally, Surface Mining management had not ensured that the warning message for unauthorized use was displayed as the first screen seen by a user.

Effect: Without adequate controls in place to ensure proper access to automated information systems, there is the risk that unauthorized access to the systems could occur, resulting in the corruption of sensitive data or systems processing and the denial of service.

ACCESS CONTROLS

Recommendations:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement:

1. Develop and implement policies and procedures establishing the maximum number of log-in attempts allowed for its automated information systems in compliance with Department of the Interior regulations.

2. Ensure that the systems log-in warning message is the first screen displayed upon initial access and prior to the user being authenticated as a valid system user.

ACCESS CONTROLS

G. Password Settings

Condition: Password requirements for accessing Surface Mining's automated information systems were inadequate. Specifically, we found that:

- Passwords did not contain a minimum number of characters or include special characters.

- Passwords were fewer than the Department's standard of six characters in length, were common words, and were the same as users' IDs.

- Passwords were not changed periodically.

- Users were allowed to bypass password length and expiration settings.

- System administration passwords were shared. In one instance, the Sun Solaris operating system was accessed over the Internet using the system administration account and password, and the password was in an unencrypted form

Furthermore, using intrusion detection software, passwords for the Sun Solaris and Windows NT operating systems and the network router were identified within a 24-hour period, and powerful system administration level account passwords were obtained.

Criteria: The National Institute of Standards and Technology's "Generally Accepted Principles and Practices for Securing Information Technology Systems" states that if passwords are used for authentication they should have attributes such as a minimum length of six characters, should include special characters, should not be in an online dictionary, and should be unrelated to the user ID. Also, the Department of the Interior's Automated Information Systems Security Handbook requires that passwords be a minimum of six characters and be changed periodically (90 days is recommended).

Cause: Surface Mining had not developed policies and procedures on creating and changing passwords for its automated information systems. In addition, Surface Mining had not developed a policy requiring system administration personnel to log on to the system under specific user IDs that were issued to each individual.

ACCESS CONTROLS

Effect: The current password settings reduce the effectiveness of the password as a control, thereby increasing the risk for unauthorized access to sensitive information through password disclosure.

Recommendations:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement:

1. Develop and implement password policies and procedures. In addition, controls to ensure compliance with these policies and procedures should be implemented.

2. Implement a policy requiring system administration personnel to log on to the automated information systems under specific user IDs.

3. Evaluate current capabilities and implement procedures to address encryption or other security methods to help prevent powerful system passwords and accounts from being compromised when traveling across a network, such as the wide area network and the Internet.

ACCESS CONTROLS

H. Novell Network Access

Condition: "Public" users had inappropriate access to computer resources on the Novell network. Specifically, "Public" users had browse access at the root,* which allowed anyone to view user IDs and gather information without logging onto the network. Also, we identified 13 accounts with null[3] passwords. In addition, the passwords were not required to be reset, which allowed anyone to log into these accounts to make unauthorized modifications or to manipulate data.

Criteria: Office of Management and Budget Circular A-130, Appendix III, requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. The Circular defines "adequate security" as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information." Also, the National Institute of Standards and Technology's "Generally Accepted Principles and Practices for Securing Information Technology Systems" states, "Organizations should implement logical access control based on policy made by a management official responsible for a particular system, application, subsystem, or group of systems."

Cause: Surface Mining management had not developed policies and procedures to ensure that only authorized users had root access and that all accounts had active passwords.

Effect: As a result, Surface Mining could not protect the Novell network operating system and other system software from unauthorized modification or manipulation and therefore could not ensure the integrity and availability of the network, the systems, and the data.

'Root provides "a person with unlimited access privileges who can perform any and all operations on the computer. Also called superuser." (The Computer Language Company, Inc., Computer Desktop Encyclopedia, 1981-1998)

'Null (null value) is "a value in a field or variable that indicates nothing was ever derived and stored in it." (The Computer Language Company, Inc., Computer Desktop Encyclopedia, 1981-1998)

ACCESS CONTROLS

Recommendation:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement, develop policies and procedures to ensure that controls are in place to protect the Novell network operating system and other system software from unauthorized modification or manipulation.

ACCESS CONTROLS

I. User Access Control

Condition: Surface Mining's Information Systems Management Office in Washington, D.C., and the Division of Financial Management in Denver, Colorado, had not implemented controls that limited access to its Novell file servers. Specifically, the "SECURE CONSOLE" command for the Novell file servers was not used. The "SECURE CONSOLE" command removes DOS from the file servers, which prevents users from shutting down the file server, exiting to DOS, and running unauthorized programs. Also, the "LOCK CONSOLE" command was not used. The "LOCK CONSOLE" command ensures that only users with proper authorization can access the file servers. Additionally, the password for the "RCONSOLE" was not encrypted[4] and resided in at least two files (the autoexec.ncf and the netinfor.cfg) at the Division of Financial Management. The "RCONSOLE" command establishes connections that enable keyboard strokes at the workstations to be sent to the file servers and screen image changes at the file servers to be sent to remote workstations.

Criteria: Office of Management and Budget Circular A-130, Appendix III, requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. Circular A-130 defines "adequate security" as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

Cause: Surface Mining management had not identified or implemented the technical controls necessary to ensure that only authorized users had access to the Novell file servers.

Effect: As a result, Surface Mining increased the risk that unauthorized individuals could access its file servers to run programs or gain access to data files. For example, because the "RCONSOLE" command was not encrypted, sensitive files could be copied to an unprotected location during maintenance/emergency procedures or be viewed by technical contractors or staff who had temporary supervisory access to the file servers.

Recommendation:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement, identify and implement the technical controls necessary to ensure that only authorized users

[4]Encrypt is to "encode data for security purposes." (The Computer Language Company, Inc., Computer Desktop Encyclopedia, 1981-1998)

ACCESS CONTROLS

have access to the Novell file servers. The controls should include using the “SECURE CONSOLE” command in the autoexec.ncf file, encrypting the “RCONSOLE” password, and using the “LOCK CONSOLE” command.

ACCESS CONTROLS

J. Network Protection

Condition: Surface Mining's Division of Financial Management did not protect its local area network against probes and attacks from unauthorized users. Specifically, the configuration of the Division's network allowed internal and external users to access the systems.

Criteria: Office of Management and Budget Circular A-130, Appendix III, requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. Circular A-130 further defines "adequate security" as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information." Additionally, the National Institute of Standards and Technology's "Executive Guide to the Protection of Information Resources" states, "Agency information should also be protected from intruders ... as well as from employees with authorized computer access privileges who attempt to perform unauthorized actions."

Cause: The Division of Financial Management did not protect its local area network because it had not implemented a firewall[5] system that defined the services and accesses to be permitted or denied when accessing its local area network. Although the Division had a router[6] in place, the router was not used as a firewall to filter access.

Effect: As a result, unauthorized users could easily gain access to the Division of Financial Management's financial and other sensitive applications. For example, the Division's network was vulnerable to passive threats, such as an intruder viewing data, and active threats, such as an intruder modifying data.

---

[5]Firewall is a "method for keeping a network secure. It can be implemented in a **single** router that filters out unwanted packets, or it may be a combination of technologies in router and hosts. They are also used to keep internal network segments secure. For example, a research or accounting subnet might be vulnerable to snooping from within." (The Computer Language Company, Inc., Comnuter Desktop Encvclonedia, 1981-1998)

[6]Router is a "device that forwards data packets from one local area network or wide area network to another. Routers are used to segment local area networks in order to balance traffic within workgroups and to filter traffic for security purposes and policy management." (The Computer Language Company, Inc., Comnuter Desktop Encvclonedia, 198 1- 1998)

ACCESS CONTROLS

Recommendation:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement, install a firewall system for the Division of Financial Management's local area network.

SYSTEM SOFTWARE CONTROLS

Control Objective: The control objective for system software is to limit and monitor access to the powerful programs and sensitive files that control the computer hardware and secure applications supported by the system.

K. System Audit Tools

Condition: Surface Mining management did not use available system audit tools to ensure integrity over automated information systems processing and data and to detect inappropriate actions by authorized users. For example, we found that:

- Systems audit software was not used for the Windows NT and Novell servers and the Hewlett Packard and Sun Solaris operating systems at the Divisions of Information Systems Management and Financial Management. According to the "NIST Handbook," this type of tool could assist data center and installation security management in evaluating its systems for security flaws, such as identifying security exposures related to "improper access controls or access control configurations, weak passwords, lack of integrity of the system software, or not using all relevant software updates and patches."

- Some systems options for the Windows NT servers and the Novell operating system at the Divisions of Information Systems Management and Financial Management that produce audit trails in the systems were not implemented. However, for those systems that had systems options implemented to produce audit trails, the audit trails were not reviewed periodically. In addition, in the systems that had implemented the options to maintain the audit trail, the settings allowed the systems to overwrite* the audit trail. Therefore, in some of the systems, an audit trail that logs the results of actions taken by system programmers, system administration, and system users could not be reviewed.

Criteria: Office of Management and Budget Circular A-130, Appendix III, requires agencies to establish controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems. In addition, Circular A- 130 states that individual accountability is one of the personnel controls required in a general support system. Circular A- 130 further states that an example of one of the controls to ensure individual accountability is examining or looking at patterns of users' behavior by reviewing the audit

'Overwrite is "to record new data on top of existing data such as when a disk record or file is updated." (The Computer Language Company, Inc., Computer Desktop Encyclopedia ,1981- 1998)

SYSTEM SOFTWARE CONTROLS

trails. Also, the "NIST Handbook" states that audit trails are a technical mechanism to achieve individual accountability. In addition, the "Handbook" recognizes that not taking advantage of automated tools to assist in the review of computer systems security features "puts system administrators at a disadvantage."

Cause: Surface Mining management did not (1) require systems integrity and verification software, (2) implement systems options to record actions taken affecting systems controls and processing, (3) use and maintain available systems audit trails to detect and identify inappropriate actions affecting the systems processing and data integrity, and (4) establish procedures requiring periodic reviews of resultant systems logs.

Effect: As a result, inappropriate systems settings and processing were not identified and recorded. Additionally, without periodic reviews of system audit trails, there was an increased risk that processing problems or unauthorized activities would not be detected or would not be detected timely and that the individual responsible would not be held accountable for the inappropriate actions.

Recommendations:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement:

1 Evaluate acquiring systems verification and auditing software.

2. Implement the systems options available in each of the operating systems to record activities affecting the systems.

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

4. Develop and implement procedures to ensure that periodic reviews of systems logs for unauthorized or inappropriate activities are performed and that unauthorized or inappropriate activities are reported to Surface Mining management.

SYSTEM SOFTWARE CONTROLS

L. System Software Vulnerabilities

Condition: Surface Mining did not have adequate controls to ensure that necessary system software updates were implemented in a timely manner. Specifically, service packs[9] available in October 1998 to address vulnerabilities in the Windows NT operating system had only been implemented by the Division of Financial Management in two of the four NT systems affected by the vulnerabilities as of March 30, 1999.

Criteria: Federal Information Processing Standards Publication 106, "Guideline on Software Maintenance," states that "software maintenance is the performance of those activities required to keep a software system operational and responsive after it is accepted and placed into production." In addition, the "Guideline" states that "software maintenance is the set of activities which result in changes to the originally accepted (baseline) product set." Further, the "Guideline" states that "these changes are made in order to keep the system functioning in an evolving, expanding user and operational environment."

Cause: Surface Mining management had not established policies and procedures to ensure that current service packs to the operating systems were evaluated for implementation and that the current fixes available from the vendor to address systems problems and vulnerabilities were implemented when necessary.

Effect: The risk is increased that known operating systems vulnerabilities that have been identified and addressed by the systems software vendor will not be implemented by Surface Mining management as necessary.

Recommendations:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement:

1. Establish policy and procedures for ensuring that available software updates and service packs are reviewed to identify those that should be implemented to address an applicable systems vulnerability.

2. Implement procedures to ensure that those updates which are determined to be needed are implemented in a timely manner.

---

[9]Service packs is "a software patch that is applied to an Installed application. It is typically downloaded from the vendor's Web site. When executed, it modifies the application in place." (The Computer Language Company, Inc., Desktop Encyclopedia, 1981-1998)

SEPARATION OF DUTIES

Control Objective: The control objective for separation of duties is the establishment of policies, procedures, and organizational structure so that one individual cannot control key aspects of computer-related operations and thereby conduct unauthorized actions or gain unauthorized access to assets or records.

M. Duties Related to Automated Information Systems

Condition: The duties related to all the automated information systems throughout Surface Mining were not separated effectively. Specifically, we found that:

- Individuals responsible for setting up users of the automated information systems were also the individuals controlling the systems security logs that record the activities of the users of these systems.

- Individuals who controlled systems audit trails were also responsible for system administration, which resulted in these personnel monitoring their own system activities.

- Application programmers who made code changes to software were also responsible for moving those changes into production.

- Application programmers were responsible for changing production data.

Criteria: Office of Management and Budget Circular A-130, Appendix III, requires that security controls of personnel include separation of duties. Circular A- 130 and the "NIST Handbook" define separation of duties as the division of roles and responsibilities and of steps in a critical function so that no one individual can undermine a critical process. Additionally, Surface Mining's Information Resources Management (IRM) Policies and Procedures Manual states that appropriate safeguards should be used "to prevent unauthorized access to and use of information, data, and software." The "Generally Accepted Principles and Practices for Securing Information Technology Systems," issued by the National Institute of Standards and Technology, states, "In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification." This publication further states that "access to online audit logs should be strictly controlled" and that "[o]rganizations should strive for separation of duties between security personnel who administer the access

SEPARATION OF DUTIES

control function and those who administer the audit trail." Additionally, the publication states that "audit trails should be reviewed periodically."

Cause: Surface Mining management had not ensured that personnel whose duties included performing reviews of security logs were different from the personnel whose responsibilities included establishing users on those systems. In addition, no policy had been implemented to ensure that systems audit trails were maintained and controlled by individuals other than those individuals responsible for administration of the access control function. Further, the Division of Financial Management did not appropriately assign duties for application programmers to ensure that critical processes were not subverted. Specifically, application programmers should not have access to production data because production data should be restricted to users.

Effect: Since logging and subsequently reviewing the logs are primary detection controls used to identify inappropriate activities of users who have significant system access, separating these two functions provides one of the main internal controls over the system administration function. As a result, there was an increased risk that inappropriate actions by the individuals who established system users would not be detected or would not be detected timely. In addition, there is an increased risk that accidental or intentional unauthorized actions by programmers could threaten the integrity of Surface Mining's data and disrupt systems processing.

Recommendations:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement:

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

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

SOFTWARE DEVELOPMENT AND CHANGE MANAGEMENT"

Control Objective: The control objective for software development and change management is to prevent unauthorized programs or modifications to an existing program from being implemented.

N. Change Management Controls

Condition: Change management controls over applications software were not adequate. Specifically, we found that:

- The applications implementation, conversion, and testing process was inadequate, causing data to be incorrect and requiring users to identify data errors, prepare and submit change requests to correct the data, and to reenter the correct data. Additionally, without adequate change management controls, Surface Mining was at risk of having malicious codes inadvertently or deliberately added to the applications software.

- Software edits were removed without ensuring that change management controls were followed. Thus, changes were made that were not authorized, approved, and tested.

- User change requests were not addressed in a timely manner.

Criteria: Office of Management and Budget Circular A-127, "Financial Management Systems," states, "Financial management systems shall be designed to provide for effective and efficient interrelationships between software, hardware, personnel, procedures, controls, and data contained within the system." Surface Mining's "Information Resources Management (IRM) Policies and Procedures Manual" requires system owners to establish formal, written standards for program changes (both scheduled and emergency) and to authorize all scheduled program changes. In addition, the "Manual" requires system managers to ensure that all program changes meet formal, written standards and to notify the system owner when emergency program changes are made. Also, the "Manual" requires that unit, integration, system, and acceptance testing be used when a new system is developed or an existing system is enhanced.

Cause: Surface Mining management did not ensure that its "Information Resources Management (IRM) Policies and Procedures Manual" was followed for changing applications software. Additionally, because change requests were not addressed timely, Surface Mining had a significant change request backlog that may reduce the ability of the applications meeting the users' requirements.

SOFTWARE DEVELOPMENT AND CHANGE MANAGEMENT

Effect: As a result, the risk was increased that processing irregularities or malicious codes could be introduced, data lacked integrity, and applications were not functioning to meet users' needs. In addition, the applications did not process data accurately, which resulted in insufficient and costly manual processes, such as time and personnel resources, to supplement the applications deficiencies.

Recommendations:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement:

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

2. Establish the process of correcting applications deficiencies as a high priority to reduce manual processes.

3. Review change requests timely to ensure that user requirements are supported in the applications.

SERVICE CONTINUITY

Control Objective: The control objective for service continuity is to ensure that when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected.

0. Business Continuity of Operations

Condition: Surface Mining had not developed continuity of operations plans for its telecommunications links or finalized plans for its facilities and data centers. In addition, while Surface Mining had completed draft plans for its data centers and its facilities, these plans had not been approved or tested, and training had not been provided to personnel on the plans. Further, the off-site facility (cold storage for backup tapes) for Surface Mining headquarters operations was not located at. least 1 mile from the headquarters location.

Criteria: Office of Management and Budget Circular A-130, Appendix III, requires agencies to establish a comprehensive contingency plan and periodically test the capability to perform the agency function supported by the application, as well as critical telecommunications links, in the event of a disaster or system failure. Additionally, the "NIST Handbook" states that a comprehensive disaster recovery plan is necessary to ensure the timely recovery of all business functions and the systems environment that are critical for day-to-day operations and to minimize downtime. Further, the "NIST Handbook" recognizes that personnel should be trained in their contingency-related duties. In addition, the "NIST Handbook" states that a primary contingency strategy for applications and data is storage at a secure off-site facility. According to the "NIST Handbook," a secure off-site storage facility should be physically and environmentally protected to prevent unauthorized individuals from access and to protect data from heat, cold, or harmful magnetic fields and should be located at least 1 mile from the installation. Also, the Department of the Interior "Automated Information Systems Security Handbook" mandates off-site storage for "all AIS [automated information systems] installations providing critical support to the organization's missions."

Cause: Prior to the issuance of the Department of the Interior's Office of Managing Risk and Public Safety Policy Bulletin 98-001, "Continuity of Operations Planning - Guidance and Schedules," dated March 1998, Surface Mining did not have any contingency plans for its telecommunications links, facilities, or data centers. At the time of our review, Surface Mining had developed contingency plans for its data centers and facilities, but it had not included plans for telecommunications links and had not addressed the testing of these plans. Further, Surface Mining management was unaware of the requirement

to have an off-site storage facility located at least 1 mile from the original computer facility installation.

Effect: As a result, Surface Mining increased its risk of being unable to recover and resume critical operations should the systems fail or disasters occur.

Recommendations:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement:

1. Ensure that a contingency plan is developed for critical telecommunications links.

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

3. Provide for a secure off-site storage facility that is at least 1 mile from the computer facility.

SERVICE CONTINUITY

P. Incident Response Plan and Team

Condition: Surface Mining did not have a formal incident response plan and a formal response team in place to respond timely and efficiently to information system security incidents whether an incident was caused by a computer virus, other malicious codes, or a system intruder (either an insider or an outsider). A security incident may affect sensitive systems at different network sites, including contractors and clients. For example, end users would not know whom to contact if they find or have inadvertently introduced a virus to the network. Further, the system administrators may not escalate the incident to Surface Mining's security management, thus allowing the virus to populate the wide area network.

Criteria: Office of Management and Budget Circular A-130, Appendix III, states that "when faced with a security incident, an agency should be able to respond in a manner that both protects its own information and helps to protect the information of others who might be affected by the incident. To address this concern, agencies should establish formal incident response mechanisms."

The National Institute of Standards and Technology's "Generally Accepted Principles and Practices for Securing Information Technology Systems" states that "an organization should address computer security incidents by developing an incident handling capability."

Cause: Surface Mining did not have a formal incident response plan or a formal response team because management believed that the local area and wide area network administrators were prepared to respond to each security breach based on what occurred during the incident. We believe that without a formal plan, Surface Mining may not have identified all types of incidents and actions to take to prevent further spreading of a virus. A formal incident response plan would include, for example, names of important contacts, both external and internal, such as managers and technical support personnel to aid in containment and recovery efforts and, if appropriate, Federal law enforcement officials to investigate the incidents.

Effect: Without a formal response plan and team, Surface Mining cannot provide assurance to its users, contractors, or clients that data would be protected, that security incidents would be handled quickly and efficiently, and that corrective actions would be implemented.

SERVICE CONTINUITY

Recommendation:

We recommend that the Director, Office of Surface Mining Reclamation and Enforcement, develop and implement a formal incident response plan and team.

OFFICE OF SURFACE MINING RECLAMATION AND ENFORCEMENT SENSITIVE AUTOMATED INFORMATION SYSTEMS

Office of Surface Mining's Sensitive Automated Information Systems as Reported to the Department of the Interior in Surface Mining's "Automated Information Systems Security Plan," Dated February 1998

Advanced Budget/Accounting Control and Information Systems (ABACIS)
Audit Fee Billing and Collection System (AFBACS)
Abandoned Mine Lands Inventory System (AMLIS)
Applicant Violator System (AVS)
Civil Penalty Accounting Control System (CPACS)
Coal Data Repository System (CDR)
Electronic Mail (E-Mail)
Fee Billing and Collection System (FEEBACS)
Grants Information Fund Tracking System (GIFTS)
Litigation Tracking System (LTS)
Payroll/Personnel Data Entry (PAY/PERS)*
Synergistic Acquisition Tracking Inventory Network (SATIN)
Technical Information Processing System (TIPS)

Additional Sensitive Systems**

Correspondence Tracking System (CTS)
Office of Surface Mining Wide Area Network (OSMNET)
Work Assignment Tracking System/Mine Information, Project Planning System (WATTS/MIPPS)
Administrative Records Management System (ARMS)

*In its response to the draft report, the Office of Surface Mining stated that this system "is no longer used."

**In its response to the draft report, the Office of Surface Mining identified additional mission critical or sensitive systems.

OFFICE OF SURFACE MINING
RESPONSE TO IG AUDIT RECOMMENDATIONS
September 17, 1999

OSM reviewed the Draft Audit Report and agrees that we must have documented security plans, risk analysis, and a security policy. Although many of our security procedures were not written in these specific documents, we do have security controls in place. The Division of Financial Management operates sensitive systems which process financial data. These systems are comprised of two computer platforms, the Hewlett-Packard and the SUN, which operate seven of the 16 Mission Critical Systems in OSM.

To ensure that the operating environment at the Division of Financial Management is secure and that the financial systems are protected, we maintain a secure building that houses the computer systems. The computer room contains an un-interruptible power supply and is environmentally controlled with an "automated notification" temperature and electrical monitor. In addition, we have off-site storage of system and application back-ups which have been tested,

Security access systems are in place that limit "system administrator" privileges to the system administrator, their backup, and select other personnel on an as needed basis. We have separation of functional duties to preclude any one person from processing a transaction from beginning to end. In addition, Daily Synchronization Reports are produced to test the integrity of the data in the systems and all system modifications are tested prior to implementation.

The following responses address each of the 38 recommendations identified in Appendix 1 of the Draft Audit Report:

SECURITY PROGRAM

A. Risk Assessments

Recommendations:

1. **Determine the risks associated with each of the systems and, based on the results of the risk assessments, establish appropriate security policies and procedures.**

Response: OSM concurs with tliis recommendation and offers the following response:

OSM completed a risk assessment for each of its 16 mission critical systems and has established security policies and procedures. The risk assessments for each of the OSM's mission critical systems are at attachment I. The security policies and procedures are at attachment II.

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

Response: OSM concurs with this recommendation and offers the following response:

The risk assessments developed by OSM, were conducted in accordance with Federal Guidelines and document the acceptance of risk and the selection of appropriate controls. A copy of these risk assessments are at attachment I. The IG has conducted an interim review of several of these risk assessments and given OSM recommendations for improvements, and these recommendations are being incorporated into the completed final risk assessments.

3. **Formally assign and communicate responsibility to those required to participate in assessing risks.**

Response: OSM concurs with this recommendation and offers the following response:

The Information Systems Security Officer (ISSO) has been formally assigned as the security officer for OSM, and is responsible for ensuring that continuing risk assessments are performed on OSM's mission critical systems. The Information System Security Officer has contacted each of the systems owners of OSM's 16 mission critical systems and had them participate in developing the risk assessments at attachment I. Chapter I of the Security Directive provides policy concerning the Program Managers responsibility for creating and implementing security plans and risk assessments for mission critical systems in their area of responsibility.

SECURITY PROGRAM

B. System Security Plans

Recommendations:

1. **Provide resources to ensure that automated information systems security plans are developed for its general support systems and major applications in accordance with the Computer Security Act; Office of Management and Budget Circular A-130, Appendix III; and the National Institute of Standards and Technology Special Publication 800-18.**

Response: OSM concurs with this recommendation and offers the following response:

OSM has provided the necessary resources and developed system security plans for each of its mission critical systems. The security plans for each of OSM's 16 mission critical systems are at attachment III. There is one automated system on your list of mission critical systems that should be removed. The Payroll/Personnel Data Entry (PAY/PERS) is no longer used by OSM. The IG conducted an interim review of several of these security plans and has given **OSM** recommendations for improvements. These recommendations are being incorporated into the completed security plans.

2. **Ensure that the automated information systems security function is elevated organizationally to report directly to Surface Mining's Chief Information Officer and formally provide the position with the authority to implement and enforce the Surface Mining-wide computer security program.**

Response: OSM concurs with the recommendation that the security function should be elevated, however we feel that it should be elevated to the Deputy Chief Information Officer rather than the Chief Information Officer, for the following reason:

The Deputy Director of OSM is designated as Chief Information Officer for the Bureau. *However,* at the present time, OSM does not have a Deputy Director. Therefore, OSM will elevate the security function organizationally to report directly to the Deputy Chief Information Officer.

3. **Report the lack of security plans for surface mining's 13 sensitive systems as material weakness in Surface Mining's annual assurance statement on management controls for fiscal year 1999.**

Response: OSM concurs with the finding that there was a lack of security plans for 13 sensitive systems. However, OSM does not feel that this should be reported as a material weakness in the annual assurance statement on management controls for fiscal year 1999, for the following reason:

OSM has completed security plans for all of it's 16 mission critical systems. These security plans are at attachment III.

SECURITY PROGRAM

C. Security-Related Personnel Policies and Procedures

Recommendations:

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

Response: OSM concurs with this recommendation and offers the following response:

OSM has developed a Security Directive (copy at attachment II), which contains personnel security policies and procedures for obtaining appropriate security clearances for personnel filling sensitive and critical trust positions. In addition, the Office of Personnel has developed a procedures guidelines document, which has been included in Chapter VI of the Security Directive, that will provide guidance on how to designate position sensitivity for all OSM positions, and the level of background investigations which should be completed on each type of position.

The Office of Personnel is in the process of identifying all personnel in Sensitive Computer Areas and their position risk designation to assure proper clearance and background investigations are completed. The procedures for implementing this policy is found in Chapter VI of the Security Directive.

2. **Ensure that all automated data processing contractor employees have proper background clearances.**

Response: OSM concurs with this recommendation and offers the following response:

OSM has developed mandatory language to be used in all agency contracts requiring that all contractor employees receive proper background clearances. This language will be in all agency contracts effective with contract renewals for October 1, 1999. In addition to mandatory language in all agency contracts, all contractors currently on-board will receive a background clearance, if required, and the requirement for all new contractor employees to receive proper background clearances is included in the OSM Security Directive at attachment II, in Chapter I, Section E.

3. **Ensure that periodic re-investigations are completed every 5 years on personnel who are in public trust high risk positions.**

Response: OSM concurs with this recommendation that periodic re-investigations should be completed on personnel in public trust high risk positions and offer the following response:

OSM agrees that re-investigations should be completed on personnel in public trust high risk positions. Although we are a small agency with few resources for re-investigations, we will ensure that periodic re-investigations are completed every five years on personnel in public trust high risk positions. Chapter VI contains policy on OSM's Personnel Security Program.

ACCESS CONTROLS

D. **Resource classifications**

Recommendation:

1. **We recommend that the Director, Office of Surface Mining Reclamation and Enforcement, develop and implement policies to classify Surface Mining's computer resources in accordance with the results of periodic risk assessments and guidance contained in Office of Management and Budget Circular A-130 Appendix III,**

Response: OSM concurs with this recommendation and offers the following response:

OSM has completed risk analyses and security plans for all sensitive systems, which will be approved by appropriate agency personnel in concert with Program Managers. The Security Directive at attachment II includes policy on how to designate sensitive data and requirements for sensitive and non-sensitive data. In addition, OSM has developed and implemented policies in the OSM Security Directive to ensure that access controls are in place that limit access to Sensitive Computer Areas to protect computer resources from unauthorized modifications, loss, disclosure or compromise.

E. Access Levels

Recommendations:

1. **Institute a policy of "least privilege" access levels to ensure that access to resources and data is limited to those users who require such access.**

Response: OSM concurs with this recommendation and offers the following response:

In Chapter XII, Section D of OSM's Security Directive, at attachment II, policy has been included to ensure that access to resources and data is limited to those users who require such access. The Division of Financial Management completes a total review of all User access privileges every six months. This involves the system owners reviewing all employees who have access to their applications and related assigned privileges.

2. **Develop and implement policies and procedures for approving access to the automated information systems that include the formal assignment of responsibility for approving sys tern access.**

Response: OSM concurs with this recommendation and offers the following response:

OSM has written policies and procedures in Chapter XII, Section D of the Security Directive for approving access to the automated information systems and has assigned responsibility for approving systems access to the appropriate areas within the organization. OSM requires that all requests for User ID's and access privileges by DFM users be documented

via a hardcopy authorization form or electronic request with proper approval by system owners.

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

Response: OSM concurs with this recommendation and offers the following response:

OSM has included procedures in Chapter XII, Section D of the Security Directive that user access levels are periodically reviewed to ensure that access levels provided are appropriate. OSM requires that all system administrators complete a total review of all User access privileges every six months. This involves the system owners reviewing all employees who have access to their applications and related assigned privileges.

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

Response: OSM concurs with this recommendation and offers the following response:

The OSM Employee Exit Clearance Form will be updated to include a section for the supervisor of the employee being reassigned or terminated to sign. The signature will remind the supervisor of his responsibility to immediately notify the Information Systems Security Officer that a particular employee has had a change of status. In addition, as an increased security precaution, the Office of Personnel will send a message to the systems administrators listing all employees that have left the agency during the previous pay period. This policy is in Chapter IX, Section B.

5. **Implement controls to ensure that system owners approve all access to their application in accordance with Surface Mining Policy.**

Response: OSM concurs with this recommendation and offers the following response:

The OSM Security Directive, attachment II, Chapter IX, Section B, contains policy requiring system owners to approve all access to their application systems. OSM requires that all requests for User ID's and access privileges be documented via a hardcopy authorization form or electronic request with proper approval by system owners. Before user-id's generated as a result of these requests are activated, DFM must receive a signed "Rules of Behavior" from the user.

F. **System Log-in**

Recommendations:

1. **Develop and implement policies and procedures establishing the maximum log-in attempts allowed for it automated information systems in compliance with Department of Interior regulations.**

Response: OSM concurs with this recommendation and offers the following response:

OSM has implemented policy in its Security Directive that establishes the maximum unsuccessful log-in attempts to be three (3) before the user is locked out of the system. However, the SUN computer at DFM is set for five (5) attempts prior to invalidation of a User ID, because this is a standard for the SUN Solaris System. This policy is in Chapter XII, Section D.

2. **Ensure that the systems log-in warning message is the first screen displayed upon initial access and prior to the user being authenticated as a valid system user.**

Response: OSM concurs with the recommendation and offers the following response:

The hardware and operating system architecture of the systems does not always allow a warning message to be the first screen displayed upon initial access to the system. However, OSM will place systems log-in warning message as close to the first screen as the hardware and software will allow.

G. Password Settings

Recommendations:

1. **Develop and implement password policies and procedures. In addition, controls to ensure compliance with these policies and procedures should be implemented.**

Response: OSM concurs with the recommendation and offers the following response:

OSM has included password policy and other access control measures in the Security Directive. The policy requires a minimum of six alphanumeric characters on passwords. The system software has been modified to not accept a password of less than the minimum required characters. This policy is in Chapter XII, Section B of the Security Directive.

2. **Implement a policy requiring system administration personnel to log on to the automated information systems under specific user ID's.**

Response: OSM concurs with the recommendation and offers the following response:

The OSM Security Directive, at attachment II, contains policy requiring system administrators to have and use their own unique password when logging into the systems as an administrator. This policy specifically states that system administrators are not to share

passwords. In addition, the policy states that passwords will be changed every 90 days .This policy is in Chapter XII, Section B of the Security Directive.

3. **Evaluate current capabilities and implement procedures to address encryption or other security methods to help prevent powerful system passwords and accounts from being compromised when traveling across a network, such as the wide area network and the internet.**

Response: OSM concurs with the recommendation and offers the following response:

Upon implementation of the Firewall at DFM during the fall of 1999, encryption software will be installed on client work stations belonging to the various System Administrators within the DFM to provide increased security for their user id's and passwords during transmittal.

H. Novel Network Access

Recommendation:

1. **We recommend that the Director, Office of Surface Mining Reclamation and Enforcement, develop policies and procedures to ensure that controls are in place to protect the Novell network operating systems and other system software from unauthorized modification or manipulation.**

Response: OSM concurs with this recommendation and offers the following response:

1. OSM has included policy in the Security Directive to ensure that users are not given inappropriate access to computer resources on the Novell network. Users will not be given browse access at the root, and the Security Directive (copy at attachment II), will not allow the use of null passwords. This policy is in Chapter XII, Section D.

I. User Access Control

Recommendation:

1. **We recommend that the Director, Office of Surface Mining Reclamation and Enforcement, identify and implement the technical controls necessary to ensure that only authorized users have access to the Novell file servers. The controls should include using the "SECURE CONSOLE" command in the autoexec.ncf file, encrypting the "RCONSOLE" password and using the "Lock Console" command.**

Response: OSM concurs with the recommendation that only authorized users should have access to the Novell file servers, and offers the following response:

1. The Security Directive will include policy that requires the use of encrypting the "RCONSOLE" password. In addition, the policy will also require that "SECURE CONSOLE" command in the autoexec.ncf file, and the "LOCK CONSOLE" command must be used, unless the computer room is secure, and unauthorized users are not able to gain access to the computer room. This policy is in Chapter XII, Section B.

J. *Network* **Protection**

Recommendations:

1. **We recommend that the Director, Office of Surface Mining Reclamation and Enforcement, install a firewall system for the Division of Financial Management local area network.**

Response: OSM concurs with this recommendation and offers the following response:

A firewall is currently being installed at the Division of Financial Management in Denver, and in the Headquarters location in Washington, D.C.

SYSTEM SOFTWARE CONTROLS

K. System Audit Tools

Recommendations:

1. **Evaluate acquiring systems verification and auditing software.**

Response: OSM concurs with this recommendation and offers the following response:

OSM will establish a team from its group of Information Technology resources to evaluate acquiring systems verification and auditing software. This team will be established during the agency-wide IRM Coordinators meeting being conducted in November, 1999.

2. **Implement the systems options available in each of the operating systems to record activities affecting the system.**

Response: OSM concurs with this recommendation and offers the following response:

Both the SUN and HP computer systems at DFM maintain and retains system logs for a period of six months. The audit function on both NT and Novell in other locations are enabled.

3. **Implement policies and procedures to ensure that system logs are used and are**

maintained for an **appropriate amount of time to provide an adequate audit trail of systems activities and are controlled by personnel independent of the systems access control administration function.**

Response: OSM concurs with this recommendation and offers the following response:

Both the SUN and HP computer systems at DFM maintain and retains system logs for a period of six months. The audit function on both the NT and Novell servers in Washington are enabled.

4. **Develop and implement procedures *to* ensure that periodic reviews of systems logs for unauthorized or inappropriate activities are performed and tbat unauthorized or inappropriate activities are reported to Surface Mining Management.**

Response: OSM concurs with this recommendation and offers the following response:

System administrators/system managers will review logs periodically and report incidents in conformance with OSM's Incident Reporting Procedures. The Incident Reporting Procedures are in Chapter XI, Section G of the Security Directive.

L. System Software Vulnerabilities

Recommendations:

1. **Establish policy and procedures for ensuring that available software updates and service packs are reviewed to identify those that should be implemented to address and applicable systems vulnerability.**

Response: OSM concurs with this recommendation and offers the following response:

OSM has established policy to ensure that available software updates and service packs are reviewed to identify needed software upgrades and new service packs. The DFM Quality Assurance Log schedules a monthly task to hardware system managers to check via the Internet for software upgrades and new service packs.

The system manager, based on their research and needs, will decide on implementing software upgrades. This policy is in Chapter XI, Section H of the Security Directive.

2. **Implement procedures to ensure that those updates deemed needed are implemented in a timely manner.**

Response: OSM concurs with this recommendation and offers the following response:

The DFM Quality Assurance Log schedules a monthly task to hardware system managers to check via the Internet for software upgrades and new service packs. The system manager, based on their research and needs, will decide on implementing software upgrades. This policy is in Chapter XI, Section H of the Security Directive.

SEPARATION OF DUTIES:

M. Duties Related to Automated Information Systems

Recommendations:

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

Response: OSM concurs with the recommendation and offers the following response:

DFM has procedures in place to ensure that personnel who perform access control administration are not the same individuals who review and control systems security logs and systems audit trails. Procedures of this type are handled outside of the particular software system, because hardware and software providers (Hewlett-Packard, SUN, NOVELL, and NT included) established access to system security logs, system audit trails, and the ability to create and modify user access to their computer platforms as a function of the System Manager.

In order to better control these functions, DFM has implemented a number of "checks and balances" to ensure integrity. The establishment of a new user or the modification of an existing user must be requested by the users supervisor and approved by the system owner. Then, DFM's Information Systems Security Officer coordinates with the appropriate System Manager to create or modify the user's access to the system. Biannually, the system owners reviews a list of registered users and their access levels to confirm that they are valid. This creates both a "separation of duties" between those individuals who authorize access and those individuals who enable access to DFM systems and provides for a continuing re-evaluation of access to DFM systems.

With regard to the review of control systems security logs, system software monitors unauthorized access attempts to DFM systems, and automatically disables a user ID after three to five access attempts, depending on the system specifications. This software also maintain logs of successful access to DFM systems. Logs are also reviewed by the system owner and the Information Systems Security Officer periodically to determine if unauthorized access attempts to DFM systems are being attempted.

DFM defines systems audit trails as database logs. These database logs are controlled by

the individual database administrators. Database logs are used by DFM for two purposes: (1) to identify invalid or inappropriate changes to data within DFM systems, and (2) to recover data whenever a hardware or software error occurs. Because these logs are controlled by the-database administrator and not the System Manager, the requirement for separation of duties is satisfied.

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

Response: OSM concurs with this recommendation and offers the following response:

DFM's computer programmers have the capability to check production software in and out of the application so&are libraries and to modify production data. This is a very typical process in small data processing shops. DFM does not have funding or staffing levels to maintain independent software librarians, security officers, security maintenance personnel and programmers who only work on test areas and do not have access to production areas.

Change control procedures are used by the system owner and technical staff in requesting and completing changes (STR and DSR). Programmers are assigned tasks, the systems owner tests the programmers modifications, and the programmer schedules and implements the modifications after a successful test and approval by the system owner. All program modifications are recorded via system logs, table/file date stamping, and in the DSR/STR System.

Quality and internal controls are completed via external reconciliation, quality assurance, internal control reports, and via separation of functional duties to preclude a transaction from being completed from beginning to end by one person.

SOFTWARE DEVELOPMENT AND CHANGE MANAGEMENT

N. Change Management Controls

Recommendations:

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

Response: OSM concurs with this recommendation and offers the following response:

OSM will enforce its policies and procedures to ensure that all application program modifications are properly authorized, tested, and approved and that access to and distribution of programs are controlled. This policy is in Chapter XII, Section H and Chapter IV, Section D of the Security Directive.

2. **Establish the process of correcting applications deficiencies as a high priority to reduce manual processes.**

Response: OSM concurs with this recommendation and offers the following response:

DFM has a process for prioritization of System Trouble Reports (STR) and Data System Request (DSR). All requests for changes to the systems are recorded on these forms, STR's are corrected immediately. DSR's are generated by users to improve reports, develop new reports, develop new modules, etc. We encourage users to prepare a DSR for all desired changes so that system owners can maintain an inventory of requested changes and prioritize the top five requests, Our current inventory is larger because of the resource drain by Year 2000, standard general ledger and budget object class changes.

The DFM Quality Assurance Log has an event scheduled every two weeks that requires a review and prioritization of STR/DSR. This process to correct deficiencies will be established as a high priority.

3. **Review Change request timely to ensure that user requirements are supported in the applications.**

Response: OSM concurs with this recommendation and offers the following response:

The DFM Quality Assurance Log has an event scheduled every two weeks that requires a review and prioritization of STR/DSR. This process to correct deficiencies will be established as a high priority. OSM will provide timely review of change request to ensure that user requirements are supported in a timely manner.

SERVICE CONTINUITY

0. Business Continuity of Operations

Recommendations:

1. **Ensure that a contingency plan is developed for critical telecommunications links.**

Response: OSM concurs with the recommendation and offers the following response:

OSM has developed a Continuity of Operations Plan (copy at attachment VI), which documents the re-establishment of critical telecommunications services, including telecommunications data links, within "Appendix F", Telecommunications Services. For example, DOINET, FTS2000 (AT&T), FTS2001 (MCI-Worldcorn), and the General Services Administration's local exchange carriers' service contracts stipulate loss-of-service recovery time periods by the carriers and the capability to reroute service-outage access.

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

Response: OSM concurs with the recommendation and offers the following response:

The OSM Continuity of Operations Plan documents both severity of operational outages and the respective operational contingency site locations. For example, outages affecting only the South Interior Building are to be operationally restored from the Main Interior Building in Washington, D.C. Personnel training, test-plan reviews, test-execution, and lessons learned will be incorporated and updates will be addressed annually.

3. **Provide for a secure off-site storage facility that is a least 1 mile from the computer facility.**

Response: OSM concurs with this recommendation and offers the following response:

OSM Headquarters, in Washington, D.C., has established the Appalachian Regional Coordinating Center in Greentree, Pennsylvania, a distance of more than l-mile as the secure off-site storage location.

P. Incident Response Plan and Team

Recommendation:

1. **We recommend that the Director, Office of Surface Mining Reclamation and Enforcement, develop and implement a formal incident response plan and team.**

Response: OSM concurs with this recommendation and offers the following response:

OSM is included in the letter of agreement between the Department of the Interior and the Federal Computer Incident Response Capability Program. A copy of this Letter of Agreement is at attachment V. This Letter of Agreement provides Department-wide protection for dealing with criminal activities that pose a threat to critical Federal Information Systems.

STATUS OF AUDIT REPORT RECOMMENDATIONS

Finding/Recommendation Reference	Status	Actions Reauired
A.1	Management concurs; additional information needed.	Provide an action plan that addresses the risk assessments for the four mission critical systems that were not included in the response, and include target dates and titles of the officials responsible for implementation.
A.2, A.3, B.1, B.2, C.l, C.2, C.3, D.1, E.1, E.2, E.3, E.4, ES, F.l, F.2, G.l, G.2, G.3, H.1, I.1, J.l, K.4, L.l, L.2, N.1, N.3, and 0.1	Management concurs; additional information needed.	Provide target dates and titles of the officials responsible for implementation.
B.3	Resolved.	We agree with the actions taken.
K.1	Resolved; not implemented.	No further response to the Office of Inspector General is required. The recommendation will be forwarded to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.
K.2, M.1, M.2, N.2, 0.2, 0.3, and P.l	Implemented.	No further response is required.
K.3	Management concurs; additional information needed.	Provide an action plan for developing and implementing policies and procedures to ensure that the system logs are used and that the logs are controlled by personnel independent of the system access control administration function. The plan should include a target date and title of the official responsible for implementation.

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

Internet Complaint Form Address

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

Within the Continental United States

U.S. Department of the Interior
Office of Inspector General
1849 C Street, N.W.
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) 235-922 1

Pacific Region

U.S. Department of the Interior
Office of Inspector General
Guam Field Office
4 15 Chalan San Antonio
Baltej Pavilion, Suite 306
Agana, Guam 96911

(67 1) 647-6060

HOTLINE

U.S. Department of the Interior
Office of Inspector General
1849 C Street, NW
Mail Stop 5341- MIB
Washington, D.C. 20240-000 1

Toll Free Number
l-800-424-508 1

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