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

AUDIT REPORT

FOLLOWUP OF RECOMMENDATIONS FOR IMPROVING GENERAL CONTROLS OVER AUTOMATED INFORMATION SYSTEMS, BUREAU OF INDIAN AFFAIRS

REPORT NO. 99-I-454
JULY 1999

A-I-N-BIA-002-98-M

United States Department of the Interior

OFFICE OF INSPECTOR GENERAL
Washington. D.C. 20240

JUL 26 1999

AUDIT REPORT

Memorandum

To: Assistant Secretary for Indian Affairs

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

Subject: Audit Report on Followup of Recommendations for Improving General Controls Over Automated Information Systems, Bureau of Indian Affairs (No. 99-I-654)

INTRODUCTION

This report presents the results of our audit of the implementation of recommendations contained in our April 1997 audit report titled "General Controls Over Automated Information Systems, Operations Service Center, Bureau of Indian Affairs" (No. 97-I-771) and our June 1998 audit report titled "Followup of General Controls Over Automated Information Systems, Operations Service Center, Bureau of Indian Affairs" (No. 98-I-483). The objective of our audit was to determine whether the Bureau of Indian Affairs had satisfactorily implemented the recommendations made in our prior audit reports and whether any new recommendations were warranted. This audit supports the Office of Inspector General's opinion on the financial statements of the Bureau and the Office of the Special Trustee for American Indians by evaluating the reliability of the general controls over computer-generated data that support the Bureau's and the Office of the Special Trustee's financial statements.

BACKGROUND

The Bureau's Office of Information Resources Management, through its Operations Service Center, both located in Albuquerque, New Mexico, is responsible for administering the general controls over the Bureau's and the Office of the Special Trustee's automated information systems. The Center provides computer services such as communications networks, software development, operations, and maintenance; systems recovery; and user support. The Center operates a Unisys server that is used to run the Office of the Special Trustee's applications, such as the Individual Indian Monies, and Bureau applications that support Indian trust fund accounts. The Center also operated an IBM mainframe computer until December 1997, when the Bureau transferred its IBM operations and data processing functions to a host IBM mainframe computer owned by the U.S. Geological Survey's Enterprise Data Service Center, located in Reston, Virginia. The Geological Survey's IBM computer is used to run Bureau applications, such as the Land Records Information System and the National Irrigation Information Management System.

SCOPE OF AUDIT

Our audit included an evaluation of actions taken by Bureau management to implement the 12 recommendations contained in our April 1997 audit report and the 8 recommendations contained in our June 1998 audit report and a review of the general controls in place during fiscal year 1998. To accomplish our objective, we interviewed personnel at the Operations Service Center of the Bureau's Office of Information Resources Management, contractor personnel, and personnel at the Geological Survey's Enterprise Data Service Center. We reviewed the Bureau's policies and procedures as they related to the Bureau's computer operations, analyzed system security, and reviewed and tested implementation of the prior audit reports' recommendations. Because the highest priority ofCenter personnel at the time of our review was remedying applications for year 2000 (Y2K) compliancy, the availability of Center personnel was limited. Therefore, we performed limited testing of controls over the Unisys server.

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

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

RESULTS OF AUDIT

We concluded that the general controls over the Bureau of Indian Affairs automated information systems were ineffective in the areas of its security program, access controls, software development and change controls, segregation of duties, and continuity of service. The Bureau continued to have ineffective general controls because Bureau management had not ensured that the recommendations contained in our April 1997 and June 1998 audit reports were implemented (see Appendices 1 and 2, respectively). Specifically, of the 20 recommendations from our prior audit reports, the Bureau had implemented 3 recommendations and had partially implemented 6 recommendations, but it had not implemented the remaining **11** recommendations. Office of Management and Budget Circular A- 123, "Management Accountability and Control," states:

> **Resolution of Audit Findings and Other Deficiencies.** Managers should promptly evaluate and determine proper actions in response to known deficiencies, reported audit and other findings, and related recommendations. Managers should complete, within established time frames, all actions that correct or otherwise resolve the appropriate matters brought to management's attention. ... Correcting deficiencies is an integral part of management accountability and must be considered a priority by the agency. [Managers are required to report in their annual integrity report to the President and the Congress any significant deficiencies and related risks.]

In addition, Circular A-123 states that deficiencies which are significant should be considered a "material weakness." It further states that deficiencies are significant when the management controls (1) do not provide assurance that assets are safeguarded against waste, loss, unauthorized use, or misappropriation and (2) are not adequate to protect the integrity of Federal programs or to ensure that resources are used consistent with the agency's mission; laws and regulations are followed; and reliable and timely information is obtained, maintained, reported, and used for decision making.

Additionally, publications of the Office of Management and Budget and the National Institute of Standards and Technology require Federal agencies to establish and implement management and internal controls to protect sensitive information in general support' and major application systems. Office ofManagement and Budget Circular A-130, Appendix III, "Security of Federal Automated Information Resources," states:

> Agencies shall implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. Adequate security means security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This 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.

Since the recommendations from our prior audit reports have not been implemented, the Bureau is at risk of loss, misuse, modification of, or unauthorized access to the data in its automated information systems. Further, because the Bureau had not made significant

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

progress in correcting deficiencies in the general controls over its automated systems, we believe that the Bureau is not in compliance with the Federal Financial Management Improvement Act and should report these deficiencies to the Department as a material weakness in the Bureau's annual assurance statement on management controls, which is required by the Federal Managers' Financial Integrity Act.

The impact on the Bureau's general controls as a result of the Bureau's lack of implementation of the related recommendations is discussed in the sections that follow.

System Security Program

The Bureau did not have an effective system security program that included an information resource management strategic plan, periodic risk assessments, periodic assessments of the system security program's effectiveness, and personnel security policies and procedures to ensure that appropriate security clearances for personnel in sensitive or critical automated data processing (ADP) positions were obtained. We made nine recommendations relating to this weakness in the prior reports (Nos. A.1, A.2, A.3, and B.l in our April 1997 report (see Appendix 1) and Nos. A.l, A.2, A.3, A.4, and A.5 in our June 1998 report (see Appendix 2)). During our current audit, we found that the Bureau had implemented one recommendation and had partially implemented two recommendations, but it had not implemented the remaining six recommendations. Therefore, the Bureau had little assurance that its information resources were used and managed effectively to accomplish its mission or that established controls could be relied on to protect mission-based sensitive computer systems and data.

Access Controls

Physical and logical access controls over the Bureau's automated information systems were ineffective. Specifically, the Bureau did not classify its resources to determine the level of security necessary, monitor visitor activities while at the Center, perform periodic reviews to ensure that users' access levels to the mainframe computers were appropriate, and change passwords to access the Unisys computer periodically. We made six recommendations relating to this weakness in the prior reports (Nos. C. 1, D. 1, D.2, and E. 1 in our April 1997 report (see Appendix 1) and Nos. A.6 and A.7 in our June 1998 report (see Appendix 2)). During our current audit, we found that the Bureau had partially implemented two recommendations but had not implemented four recommendations. Therefore, the Bureau had little assurance that the most cost-effective access controls were in place to protect its computer resources; that the computer resources located in the Center's computer operations room, such as the mainframe computer, local area network (LAN) equipment, and daily backup tape libraries, were safeguarded from dust or fire hazards; that user access was assigned at the appropriate level; and that password controls were adequate.

Software Development and Change Controls

Software development and change controls were inadequate to ensure that the proper version of an application was used in production. For example, the programmers of the National Irrigation Information Management System and the Loan Management Accounting System not only programmed the application but also tested, authorized, and approved the movement of the modified programs from test or development into production. In addition, requests to change or modify the applications were not fully documented. We made one recommendation relating to this weakness in the prior report (No. G.l in our April 1997 report (see Appendix 1)). During our current audit, we found that the Bureau had not implemented this recommendation. Therefore, the Bureau had little assurance that only authorized programs and authorized modifications were implemented; that all programs and program modifications were properly authorized, tested, and approved; and that access to and distribution of programs were carefully controlled.

Segregation of Duties

Duties were inadequately segregated for the systems support functions in the areas of system design, applications programming, systems programming, quality assurance/testing, library management, change management, data control, data security, and data administration. We made one recommendation relating to this weakness in the prior report (No. H. 1 in our April 1997 report (see Appendix 1)). During our current audit, we found that the Bureau had partially implemented this recommendation because the IBM computer operations, such as system design and system programming, were transferred to the Geological Survey. However, the Bureau's separation of duties for system functions continued to be inadequate in the areas of applications programming, quality assurance/testing, library management, change management, data security, and data administration. Therefore, the Bureau had little assurance that programmers were making only authorized program changes; that computer programmers were independently writing, testing, and approving program changes; or that errors or illegal acts would be detected or detected timely.

Service Continuity

The Center did not have an effective means of recovering or of continuing computer operations in the event of system failure or disaster. Specifically, the Bureau's backup information, such as software applications and databases, was stored on-site in the Center's computer operations room rather than in an off-site storage facility. We made two recommendations relating to this weakness in the prior reports (No. J. 1 in our April 1997 report (see Appendix 1) and **No.** A.8 in our June 1998 report (see Appendix 2)). During our current review, we found that the Bureau had implemented one recommendation and had partially implemented the other recommendation. Therefore, there was no assurance that the Center would be able to recover or resume critical computer operations in the event a system failed or a disaster occurred.

Recommendation

We recommend that the Assistant Secretary for Indian Affairs report the Bureau's ineffective general controls over its automated information systems as a material weakness in the Bureau's annual assurance statement, which is required by the Federal Managers' Financial Integrity Act.

Bureau of Indian Affairs Response and Office of Inspector General Reply

In the June 3, 1999, response (Appendix 3) to the draft report from the Assistant Secretary for Indian Affairs, the Bureau concurred with the recommendation. Based on the response and subsequent discussions, we consider the recommendation resolved but not implemented. Accordingly, the recommendation will be forwarded to the Assistant Secretary for Policy, Management and Budget for tracking of implementation (see Appendix 4).

Regarding our April 1997 report, the Bureau, in its June 1999 response, included a revised corrective action plan. Based on our current audit and the Bureau's response, we consider 2 recommendations (Nos. H. 1 and I. 1) resolved and implemented and 10 recommendations (Nos. A. 1, A.2, A.3, B. 1, C. 1, D. 1, D.2, E. 1, G. 1, and J. 1) resolved but not implemented. Accordingly, the updated information on the prior recommendations will be forwarded to the Assistant Secretary for Policy, Management and Budget (see Appendix 5).

Regarding our June 1998 report, the Bureau, in its June 1999 response, included a revised corrective action plan. Based on our current audit and the Bureau's response, we consider three recommendations (Nos. A.l, A.3, and A.8) resolved and implemented and the remaining five recommendations (Nos. A.2, A.4, A.5, A.6, and A.7) resolved but not implemented. Accordingly, the updated information on the prior recommendations will be forwarded to the Assistant Secretary for Policy, Management and Budget (see Appendix 6).

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

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

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

SUMMARY OF RECOMMENDATIONS AND CORRECTIVE ACTIONS FOR AUDIT REPORT "GENERAL CONTROLS OVER AUTOMATED INFORMATION SYSTEMS, OPERATIONS SERVICE CENTER, BUREAU OF INDIAN AFFAIRS" (NO. 97-I-771)

Recommendations	Status of Recommendations and Corrective Actions
A. 1. The information technology security function is elevated organizationally to at least report directly to the Director, Office of Information Resources Management; is formally provided with authority to implement and enforce a Bureauwide system security program; and is provided staff to perform the required duties, such as providing computer security awareness training and performing periodic risk assessments.	Partially implemented. The Bureau of Indian Affairs stated that the Information Technology (IT) Security Manager had reported to the Director, Office of Information Resources Management, since October 1997 and that the position had Bureauwide authority for the information technology security program. The Bureau also stated that sufficient staff would be available to manage security requirements once the transfer to the host IBM computer at the U.S. Geological Survey had taken place. We found that the Security Manager reported to the Director, Office of Information Resources Management; however, we did not find that the Security Manager had acted on the authority to implement a Bureauwide security plan. Although authority is implied in the position description, the Bureau had not ensured that the Security Manager's authority was recognized by all Bureau personnel. In addition, the Security Manager is physically located at the Operations Service Center and has focused on Center security and user access to the IBM mainframe and Unisys server rather than on Bureauwide system security issues. We also found that additional staff had not been assigned to assist in providing security awareness training and performing risk assessments when the IBM operations

Recommendations	Status of Recommendations and Corrective Actions
	were transferred to the host computer at the Geological Survey.
A.2 A system security program is developed and documented which includes the information required by the Computer Security Act of 1987 and Office of Management and Budget Circular A-l 30, Appendix III, "Security of Federal Automated Information Resources," and policies and procedures are implemented to keep the system security program current.	Not implemented. The Bureau stated that it had entered into an agreement with the Geological Survey's Washington Administrative Service Center - West to develop, by July 3 1, 1998, a comprehensive security plan. The "Bureau of Indian Affairs Logical Security Internal Procedures Manual" was delivered to the Bureau during our site visit in September 1998. However, the plan was not Bureau specific but rather an overview of the Geological Survey's security for its IBM computer located in Reston, Virginia. Additionally, we found that policies and procedures were not developed and implemented to keep the system security program current.
A.3. The Bureau's security personnel perform risk assessments of the Bureau's automated information systems environment and, as appropriate, provide assurance that the necessary changes are implemented to manage the risks identified.	Not implemented. The Bureau stated that its information systems security staff would oversee this effort beginning in fiscal year 1999. However, we found that management had not developed a security program; therefore, plans had not been developed to begin risk assessments in fiscal year 1999.

Recommendations	Status of Recommendations and Corrective Actions
B. 1. Ensure that personnel security policies and procedures are developed, implemented, and enforced, including those for obtaining appropriate security clearances for personnel in sensitive or critical automated data processing (ADP) positions and for informing the security staff, in writing, whenever employees who are system users terminate their employment or are transferred.	Partially implemented. The Bureau stated that it had reorganized its position sensitivity program and that, as part of the effort, it had begun to review all sensitive positions. We found that personnel policies and procedures had not been developed or implemented to ensure that appropriate security clearances for personnel in sensitive or critical ADP positions were obtained or that security staff were notified in writing when employees terminated their employment or were transferred. However, during our site visit, the Security Manager was working with the Bureau's Central Office in reviewing the sensitivity levels of personnel assigned to the Operations Service Center. In addition, the Bureau stated that the Security Manager would ensure that the employee termination report was received and reconciled with system users. During our site visit, Bureau management had not agreed on how the termination report would be provided to the Security Manager.

Recommendations	**Status** of **Recommendations and Corrective Actions**
C. 1. Develop and implement policies to classify the Bureau'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.	Not implemented. The Bureau stated that risk assessments and classifications of its automated information systems environment would be performed beginning in fiscal year 1999 in accordance with its security program plan. According to the Bureau, assessments would be performed by teams consisting of personnel from the Bureau's Office of Information Resources Management and program offices. We found that policies which would ensure that computer resources were classified in accordance with Circular A- 130 had not been developed or implemented.
D. 1. Ensure that sufficient staff are provided to adequately monitor all visitor activities.	Not implemented. The Bureau stated that the recommendation had been implemented to the extent possible given the Bureau's available resources. The Bureau further stated that the organizational element receiving the visitors would monitor visitor activities. We found, during our site visit, that Center management did not consistently monitor visitors' activities.

Recommendations	Status of Recommendations and Corrective Actions
D.2. Ensure that funding is provided for adequate maintenance of the computer operations room, such as providing daily housekeeping services, or that fire-producing equipment and supplies are removed from the computer room.	Partially implemented. The Bureau stated that it had provided funds to the Center for full-time housekeeping and maintenance services for the computer room beginning in fiscal year 1998. We found that the Bureau had provided for daily housekeeping services and that the fire-producing equipment was no longer in use. Although housekeeping services were being performed and the fire-producing equipment identified in the prior report was no longer in use, the Center was using the computer operations room as a storage facility, which increased the risk of equipment failure and other fire hazards. For example, cardboard boxes of old records and old computer equipment were stored in the computer operations room.
E. 1. Ensure that policies are developed and implemented which match personnel tiles with system users periodically, that user identifications (IDs) are deleted from the system for users whose employment had been terminated, and that verification and approval are obtained from user supervisors and application owners or managers that the levels of access are appropriate.	Not implemented. The Bureau did not address this recommendation. We found that new or revised policies had not been developed which would match personnel tiles with system users periodically, delete user IDs from the system for users whose employment had been terminated, and ensure that verifications and approvals were obtained from users' supervisors and application owners that the users' levels of access were appropriate.
F. 1. Ensure that a higher priority is given to moving the applications that reside on the Unisys mainframe to the IBM mainframe.	Resolved. In the June 1998 audit report, we recognized that the recommendation was no longer applicable because the Bureau had determined that the Unisys applications could not be moved to the IBM mainframe.

Recommendations	Status of Recommendations and Corrective Actions
G.1. Ensure that policies and procedures are developed and implemented which clearly identify the individuals responsible and accountable for application development and changes.	Not implemented. The Bureau stated that the Applications Support Branch would develop the policies and procedures. However, we found that the Branch's highest priority was the Bureau's Y2K effort; thus, the policies and procedures had not been developed.
H. 1. Ensure that staffing at the Center is evaluated and adjusted so that duties for critical system support functions are adequately segregated and fully utilized.	Implemented. The Bureau did not address this recommendation in its responses to our prior audit reports; however, for the IBM mainframe applications, the recommendation was resolved with the transfer of the Bureau's mainframe operations to the Geological Survey's host computer. We could not verify whether the critical system support functions for the Unisys server were adjusted during our fieldwork because Center personnel were involved with the Bureau's Y2K testing and were therefore not available. Based on the Bureau's June 3, 1999, response to the draft report, we consider the recommendation implemented because the Bureau stated that it is examining organizational changes and personnel assignments to ensure that duties are separated. The Bureau further stated that it will continue to monitor its progress in separating critical system support functions.

Recommendations	Status of Recommendations and Corrective Actions
I. 1. Ensure that access and activities of the Center's system programmers are controlled and monitored by security staff and that RACF controls are established to protect system resources.	Implemented. The Bureau transferred its IBM computer operations to the Geological Survey's host computer. After the transfer, the Geological Survey established the appropriate RACF controls that would protect the system resources, which included denying the Bureau's system programmer access to the IBM computer's system controls.
J. 1. Ensure that a contingency plan is developed and tested and that funding is provided for acquiring a secure off-site storage facility.	Partially implemented. The Bureau stated that it had a disaster recovery contract which fully tested and certified the Unisys-hosted applications. However, although a contingency plan had not been developed, the Bureau had contracted for a backup site for the Unisys server in the event of a disaster and had tested the functionality of the backup site. The Geological Survey is responsible for contingency planning for the Bureau's IBM applications that reside on the Geological Survey's host computer. Additionally, although the Bureau had provided funding for off-site storage of its backup media, the Center had not used the site. The Bureau's backup media were stored on-site in the Center's computer operations room.

APPENDIX 2
Page 1 of 4

SUMMARY OF RECOMMENDATIONS AND CORRECTIVE ACTIONS FOR AUDIT REPORT "FOLLOWUP OF GENERAL CONTROLS OVER AUTOMATED INFORMATION SYSTEMS, OPERATIONS SERVICE CENTER, BUREAU OF INDIAN AFFAIRS" (NO. 98-I-483)

Recommendations	Status of Recommendations **and Corrective Actions**
A. 1. Establish as a high priority the use of the Geological Survey's host computer's operating, security, and automated job scheduling systems.	Implemented. The Bureau of Indian Affairs transferred its IBM mainframe operations to the Geological Survey's host computer in December 1997. We reported this recommendation as implemented in our June 1998 audit report.
A.2. Develop and approve an Office of Information Resources Management strategic plan that provides direction to and defines the functions of the Operations Service Center.	Not implemented. The Bureau stated that a strategic plan for the Office of Information Resources Management was being developed and finalized under a contract. The strategic plan was to have been completed by September 30, 1998. We found that the contract, dated March 9, 1998, was to support the Bureau's overall Information Resources Management strategic and tactical plans. However, contract performance was based on task orders, and at the time of our site visit, a task order had not been issued to develop a strategic plan.

Recommendations	Status of Recommendations and Corrective Actions
A.3. Hold the Information Technology (IT) Security Manager accountable for performing the position responsibilities.	Implemented. The Bureau stated that the IT Security Manager would be held accountable through the performance appraisal process. However, we found that the IT Security Manager had not been held accountable for not implementing a Bureauwide security program, providing security awareness training, or performing risk assessments. Additionally, the IT Security Manager performed the functions of a local area network (LAN) administrator, which was not part of the IT Security Manager's duties. Based on the Bureau's June 3, 1999, response to the draft report, we considered the recommendation implemented because the Bureau stated in its response that the IT Security Manager will be evaluated based on his performance standards and position description. The response further stated that the Division of Information Resources Management is in the process of "augmenting its IT security staff."

Recommendations	Status of Recommendations and Corrective Actions
A.4. Periodically perform an evaluation of the system security program's effectiveness and include any resultant corrective actions in future Bureau security plans.	Not implemented. The Bureau stated that it had entered into an agreement with the Washington Administrative Service Center **-** West to develop a comprehensive computer security plan. The plan's operating procedures and the management control reviews required by the Department of the Interior's Office of Information Resources Management would ensure that the plan would be reviewed periodically and updated. The plan was to have been developed by July 3 1, 1998. The Center received the "Bureau of Indian Affairs Logical Security Internal Procedures Manual" in September 1998. We found that the "Manual" was not Bureau specific but generally related to the Geological Survey and did not provide procedures for performing evaluations of the system security program. In addition, an evaluation of the system security program's effectiveness had not been performed in fiscal years 1996, 1997, or 1998.
AS. Redetermine, based on the Office of Information Resources Management's strategic plan, when the Bureau can begin performing risk assessments and classifying its resources. Also, personnel who will be responsible for the risk assessments and resource classifications should be identified.	Not implemented. The Bureau stated that risk assessments and classifications of its automated information systems environment would be performed beginning in fiscal year 1999 in accordance with its security program plan. However, the Bureau had not developed a security program; therefore, plans had not been developed to begin risk assessments in fiscal year **1999,** and personnel responsible for the risk assessments and resource classifications had not been identified.

Recommendations	**Status** of **Recommendations and Corrective Actions**
A.6. Obtain security clearances for ADP personnel who are not assigned to the Center that are commensurate with their positions.	Not implemented. The Bureau had begun to review and reassign security clearances for ADP personnel as a result of a Bureauwide initiative started in February 1998. During our site visit, the Security Manager was reviewing security clearances for Center personnel but had not begun to review clearances for personnel outside the Center.
A.7. Require Bureau staff to review and validate the appropriateness of users' levels of access to the Bureau's IBM applications. If the users' levels of access are not reviewed and validated by Bureau personnel, the Bureau should modify its agreement with the Geological Survey to include the requirements that access reviews and verifications should be performed for the IBM applications by the Geological Survey.	Partially implemented. Under the direction of personnel of the Geological Survey's Enterprise Data Service Center, the Security Manager had begun to review the appropriateness of users' levels of access to the Bureau's IBM applications. Although the Bureau had begun negotiations with the Geological Survey to ensure that users' levels of access were reviewed jointly by the Bureau and the Geological Survey, the Bureau had not finalized the negotiations by signing the agreement.
A.8. Remove all safety hazards from the computer operations room.	Implemented. The Bureau stated that safety hazards had been removed. During our site visit, we found that the safety hazards had been removed.

United States Department of the Interior

OFFICE OF THE SECRETARY
WASHINGTON, D.C. 20240

JUN 3 1999

Memorandum

To: Assistant Inspector General for Audits

From: Assistant Secretary - Indian Affairs

Subject: Draft Audit Report on Followup of Recommendations for Improving General Controls Over Automated Information Systems, Bureau of Indian Affairs (Assignment No. A-IN-BIA-002-98-M)

The subject audit report addresses the Bureau of Indian Affairs' implementation of recommendations made by the Office of Inspector General (OIG) in April 1977, and June 1998, audit reports on the Operation Service Center's general controls over automated information systems (Report Nos. 97-1-771 and 98-I-483, respectively). The audit found that of the 20 recommendations contained in the prior reports, the Bureau had implemented three recommendations, had partially implemented six recommendations, and had not implemented 11 recommendations. The most recent audit also includes one new recommendation.

The Bureau generally agrees with the findings of the followup audit. The revised corrective action plan (Attachment) provides information on the additional actions taken by the Bureau since the completion of the audit fieldwork and identifies revised target dates and officials responsible for implementing open recommendations.

Recommendation. [The Office of Inspector General] recommend[s] that the Assistant Secretary for Indian Affairs report the Bureau's ineffective general controls over its automated information systems as a material weakness in the Bureau's annual assurance statement, which is required by the Federal Managers' Financial Integrity Act.

Bureau Response. The Bureau concurs. The Bureau recognizes the security risks and is taking steps to correct these areas as we work to implement the recommendations made in the prior reports. The audit of the Center's general controls is conducted in conjunction with the OIG's audits of the financial statements of the Office of the Special Trustee for American Indians and of the Bureau of Indian Affairs and is used to evaluate the reliability of the general controls over computer-generated data that support these statements. As part of the corrective action, the Bureau is replacing the older applications systems with modem technology, which will enable more effective general controls over the automated systems.

The Trust Fund Accounting System (TFAS) that is being implemented by the Office of Trust Funds Management (OTFM) will replace the existing Individual Indian Monies system. Similarly, the

Bureau is implementing a Trust Asset and Accounting Management System (TAAMS) to replace the Land Titles and Records System and the Integrated Records Management System that comprise the Bureau's main Indian trust systems. Both systems will be operated and maintained by contractors. With the deployment of these two systems, the ability to prepare accurate and timely financial statements will be greatly enhanced.

Attachment

Attachment

STATUS OF CORRECTIVE ACTIONS FOR UNIMPLEMENTED RECOMMENDATIONS

OIG 97-I-771 **General Controls Over Automated Information Systems, Operations Service Center, BIA**
[Issued: April 1997]

Recommendation A. 1. The information technology security function is elevated organizationally to at least report to the Director, Office of Information Resources Management; is formally provided with the authority to implement and enforce a Bureauwide system security program; and is provided staff to perform the required duties, such as providing computer security awareness training and performing periodic risk assessments.

Status. The revised Departmental Manual chapter on BIA organization (130 DM 4) recognizes the Division of Information Resources Management (IRM) as providing Bureauwide information technology security leadership. Indian Affairs Manual (IAM) releases on information technology will also emphasize this point. To this end, IRM has evaluated the security plan for the Office of Law Enforcement. Regarding security awareness training, the Bureau is working with the Departmental information resources management staff to identify and develop LAN and Web based security awareness computer based training.

Revised Target Date:	12/31/99
Responsible Official:	IT Security Manager

Recommendation A.2. Develop and document a system security program which includes the information required by the Computer Security Act of 1987 and Office of Management and Budget Circular A-l 30, Appendix III, and implement policies and procedures to keep the system security plan current.

Status. The Bureau of Indian Affairs Logical Security Internal Procedures Manual provides a starting point for the development of a Bureauwide security plan. The security plan and the IAM issuances will provide policies and procedures for keeping the system security program current.

Revised Target Date:	12/31/99
Responsible Official:	IT Security Manager

Recommendation A.3. The Bureau's security personnel should perform risk assessments of the Bureau's automated information systems environment and, as appropriate, provide assurance that the necessary changes are implemented to manage the risks identified.

Status. It is still the Bureau's plan to initiate risk assessment in fiscal year 1999. The information security system staff will oversee the performance of the risk assessments which will be conducted in accordance with the guidance provided by OMB Circular A- 130, Appendix III, and by the General Accounting Office publication entitled "Information Security Management."

Revised Target Date:	12/31 J99
Responsible Official:	IT Security Manager

Recommendation B.l. Ensure that personnel security policies and procedures are developed, implemented, and enforced, including those for obtaining appropriate security clearances for personnel in sensitive or critical automated data processing positions and for informing the security staff, in writing, whenever employees who are system users terminate their employment or are transferred.

Status. As part of a Bureauwide effort to address deficiencies in its position sensitivity and security program, all Bureau positions were reviewed and classified consistently. The Center's IT security staff is currently working on a project to bring those background investigations current with due consideration for the levels of investigation appropriate for personnel in sensitive or critical information technology positions. Policies and procedures have been drafted, and employee checkout procedures were revised to require notification of the IT security manager as part of the employee checkout process.

Revised Target Date:	10/31/99
Responsible Official:	Bureau Security Manager

Recommendation C. 1. Develop and implement policies to classify the Bureau'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.

Status. It is still the Bureau's plan to begin the classification of its automated information systems in fiscal year 1999. The reviews will be done by IRM staff with the assistance of program personnel. This will be performed in conjunction with Recommendation A.3.

Revised Target Date:	12/31/99
Responsible Official	IT Security Manager

Recommendation D. 1. Sufficient staff are provided to adequately monitor all visitor activities.

Status. Formal procedures have been developed and issued by the Director, IRM to control visitor access into the Center. In addition, the Bureau has awarded a contract for significant improvements in access control. The improvements will include automated door control and closed circuit television subsystems.

Revised Target Date:	08/31/99
Responsible Official	IT Security Manager

Recommendation D.2. Provide funding for adequate maintenance of the computer operating room, such as providing daily housekeeping services, or remove fire-producing equipment and supplies from the computer room.

Status. The IBM 3090 and Unisys Al7 computers have been removed. The Center's daily housekeeping has been improved and the staff are no longer storing old computer equipment, records and supplies in the computer operations room. The Center has reconfigured the space to provide additional operations and storage space. This effort includes separating the area devoted to servers and tape readers from the area used for printing.

Revised Target Date:	08/01/99
Responsible Official	IT Security Manager

Recommendation E. 1. Ensure that policies are developed and implemented which match personnel files with system users periodically, that user IDs are deleted from the system for users whose employment has been terminated, and that verification and approval are obtained from user supervisors and application owners or managers that the levels of access are appropriate.

Status. The IRM is in the process of obtaining from system owners lists of individuals who have been authorized access to the respective systems. Those individuals who have not been given access have had their user identifications deleted from the systems. To date, IRM has completed this process for the Individual Indian Monies system and the Social Services Automated System. The IRM will begin reviewing the user identifications for the Land Records Information System. All other systems will be reviewed. The IRM is also in the process of comparing user identification lists with current employee lists to eliminate those individuals no longer employed by the Bureau.

Revised Target Date:	12/31/99
Responsible Official	IT Security Manager

Recommendation G. 1. Ensure that policies and procedures are developed and implemented which clearly identify the individuals responsible and accountable for application development and changes.

Status. The Applications Support Branch is responsible for developing and implementing standards, policies and procedures to ensure full accountability for all application system change management. A configuration management plan was developed for Y2K and will be expanded to cover all Bureau IT development and maintenance.

Revised Target Date:	09/30/99
Responsible Official:	Chief, Applications Support Branch

Recommendation H. 1. Ensure that staffing at the Center is evaluated and adjusted so that the duties for critical system support functions are adequately segregated and fully utilized.

Status. The Bureau recognizes that the required segregation of duties is a continuing challenge in an environment of reduced staffing levels and will continue to explore ways of ensuring separation of duties through its organizational changes and its assignments. For example, the Application Support Branch which performs and monitors system development is distinct from the security function which grants access to systems. Further, the individuals who control the data both by original data entry and data update are distinct from the Application Support Branch. The Bureau will continue to monitor the progress in this area.

Recommendation J. 1. Ensure that a contingency plan is developed and tested and that funding is provided for acquiring a secure off-site storage facility.

Status. The Center is storing its backup media at the off-site storage facility. The USGS has a disaster recovery plan for the IBM mainframe and is responsible for implementing and testing the plan. The Center has a disaster recovery plan for the Unisys system and had scheduled a test of the plan on May 3 - 4, 1999. Unfortunately, the test was postponed by the contractor. The Center is in the process of rescheduling a new test date on the plan. In addition, the Bureau is developing a Continuity of Operations plan for the Center.

Revised Target Date:	06/30/99
Responsible Official:	IT Security Manager

OIG 98-I-483 **Followup of General Controls Over Automated Information Systems, Operations Service Center, Bureau of Indian Affairs [Issued: June 1998]**

Recommendation 2. Develop and approve an Office of Information Resources Management strategic plan that provides direction to and defines the functions of the Operations Service Center.

Status. The Bureau will issue the task order for the strategic and tactical plans.

Revised Target Date:	09/30/99
Responsible Official:	Director, IRM

Recommendation 3. Hold the Information Technology Security Manager accountable for performing the position responsibilities

Status. The IT Security Manager will continue to be evaluated based upon his performance standards and position description. In addition, the IRM is in the process of augmenting its IT security staff.

Recommendation 4. Periodically perform an evaluation of the system security program's effectiveness and include any resultant corrective actions in future Bureau security plans.

Status The system security program will be periodically evaluated in accordance with the schedule established by the IT security plan and OMB Circular A-l 30. The first review will be completed and a periodic review schedule established by December 3 1, 1999.

Revised Target Date:	12/3 1199
Responsible Official:	IT Security Manager

Recommendation 5. Redetermine, based on the Office of Information Resources Management's strategic plan, when the Bureau can begin performing risk assessments and classifying its resources. Also personnel who will be responsible for the risk assessments and resource classifications should be identified.

Status. See corrective action plan for Recommendation No. A.3

Revised Target Date:	12/3 1/99
Responsible Official:	IT Security Manager

Recommendation 6. Obtain security clearances for ADP personnel who are not assigned to the Center that are commensurate with their positions.

Status Personnel in sensitive and critical automated data processing positions have been identified. Review and updating of background investigations of individuals who have IT system access and functions has been extended to include contractor employees, from coast to coast (including, for example contractor individuals in Washington, DC, and Portland, Oregon). The Bureau will continue to conduct and assure appropriate background investigations for individuals who enter the Bureau's work force and those who transfer from one role or location to another within the workforce.

Revised Target Date:	1 or3 1/99
Responsible Official:	Bureau Security Officer

Recommendation 7. Require Bureau staff to review and validate the appropriateness of users' levels of access to the Bureau's IBM applications. If the users' levels of access are not reviewed and validated by Bureau personnel, the Bureau should modify its agreement with the Geological Survey to include the requirements that access reviews and verifications should be performed for the IBM applications by the Geological Survey

Status. The Bureau will finalize the agreement with the U.S. Geological Survey to review users' level of access.

Revised Target Date:	09/30/99
Responsible Official:	Director, IRM

APPENDIX 4

STATUS OF CURRENT AUDIT REPORT RECOMMENDATION

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

STATUS OF APRIL 1997 AUDIT REPORT RECOMMENDATIONS

Finding/Recommendation Reference	Status	Action Required
H.l and I.1	Implemented.	No further action is required.
A.l, A.2, A.3, B.1, C.l, D.l, D.2, E.1, G.l, and J.l	Resolved; not implemented.	No further response to the Office of Inspector General is required. The recommendations and the revised corrective action plan will be forwarded to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.

STATUS OF JUNE 1998 AUDIT REPORT RECOMMENDATIONS

Finding/Recommendation Reference	Status	Action Required
A.l, A.3, and A.8	Implemented.	No further action is required.
A.2, A.4, A.5, A.6, and A.7	Resolved; not implemented.	No further response to the Office of Inspector General is required. The recommendations and the revised corrective action plan will be forwarded to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.

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

Internet/E-Mail Address

www.oig.doi.gov

Within the Continental United States

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

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

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

Outside the Continental United States

Caribbean Region

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

(703) 235-922 1

*North **Pacific** Region*

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

(671) 647-6060

Toll Free Numbers:
1-800-424-5081
TDD 1-800-354-0996

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

HOTLINE

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