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

# AUDIT REPORT

## FOLLOWUP OF GENERAL CONTROLS OVER AUTOMATED INFORMATION SYSTEMS, OPERATIONS SERVICE CENTER, BUREAU OF INDIAN AFFAIRS

**REPORT NO. 98-I-483**
**JUNE 1998**

# United States Department of the Interior

OFFICE OF INSPECTOR GENERAL
Washington, D.C. 20240

JUN 10 1998

# AUDIT REPORT

Memorandum

To: Assistant Secretary for Indian Affairs

From: Robert J. Williams
Acting Inspector General

Subject: Audit Report on Follow-up of General Controls Over Automated Information Systems, Operations Service Center, Bureau of Indian Affairs (No. 98-I-483)

## INTRODUCTION

This report presents the results of our followup audit 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). The objective of our followup audit was to determine whether the Bureau of Indian Affairs had satisfactorily implemented the recommendations made in our prior audit report and whether any new recommendations were warranted. This audit supports the annual financial statements audits 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 financial statements.

## BACKGROUND

The Operations Service Center is organizationally under the Bureau's Office of Information Resources Management and is located in Albuquerque, New Mexico. The Center operated an IBM and a Unisys mainframe computer and provided computer services such as telecommunications; software development, operations, and maintenance; systems recovery; and user support and is responsible for the Bureau's automated information system security. The IBM computer was used to run Bureau applications such as the Land Records Information System and the National Irrigation Information Management System. The Unisys computer was used to run Office of the Special Trustee for American Indians applications such as the Individual Indian Monies application and Bureau applications that supported the Indian trust fund accounts.

In response to our prior audit, the Bureau informed us that the IBM and Unisys mainframe computer operations and data processing functions were being transferred to a host computer owned by the U.S. Geological Survey, located in Reston, Virginia. The operating and data

processing functions provided by the Geological Survey were to allocate space on the host computer for the Bureau to operate and run its IBM operating system, applications, and security software; to provide for physical security over the host computer; to back up and recover data and files; and to provide off-site storage of backed up data and files.

## SCOPE OF AUDIT

The scope of our followup audit included an evaluation of the actions taken by Bureau management to implement the 13 recommendations made in our April 1997 audit report. In addition, we reviewed the Bureau's progress in moving the Center's mainframe data processing functions to the Geological Survey's host computer in Reston because of the impact that moving the data processing functions will have on Bureau management's ability to implement the recommendations.

This review 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. We reviewed internal controls only to the extent that they related to corrective actions taken by Bureau management on the recommendations contained in the April 1997 audit report.

# RESULTS OF AUDIT

Our April 1997 audit report concluded that the general controls over the Bureau of Indian Affairs automated information systems at the Center were not effective. Specifically, an effective security program had not been implemented; controls over access, software development and changes, segregation of duties, and system software were inadequate; and a service continuity plan had not been developed and implemented. The general controls were not effective because Bureau management had not developed a formal, up-to-date, and comprehensive system security program or established formal policies, standards, and procedures for computer operations. Additionally, the Bureau's Information Technology (IT) Security Manager* function was not at the appropriate organizational level, and adequate funding and personnel were not provided to fully support the Center's mission. The audit concluded that the deficient general controls significantly increased the risk of unauthorized access; modifications to and disclosure of sensitive data maintained in the Center's mainframe computers; theft or destruction of hardware, software, and sensitive data; and loss of critical systems and functions in the event of a disaster. In addition, the deficient controls decreased the reliability of the data maintained on the Center's computers. Our April 1997 audit report contained 13 recommendations for improving the general controls over the Bureau's automated information systems at the Center.

---

'This position was formerly known as the Bureau's Automated Information Systems Security Officer. The Departmental Manual (375 DM 19, "Information Technology Security") changed the title to "Bureau IT Security Manager."

Of the 13 recommendations made, we found that the Bureau had partially implemented 2 recommendations and had not implemented 10 recommendations and that 1 recommendation was no longer applicable because the Bureau changed its plans for the Unisys computer (see Appendix 1). Therefore, we concluded that the general control weaknesses and risks identified by our prior audit for fiscal year 1996 continued to exist during fiscal year 1997. We have made eight new recommendations to address the weaknesses we found during the followup audit.

In its response to the April 1997 audit report, the Bureau also stated that many of the weaknesses identified would be corrected with the movement of the Center's data processing functions to the Geological Survey's host computer. However, the Center will continue, at least for fiscal year 1998, to control, operate, and maintain its computer operating system and security software and to schedule production runs manually rather than use the Geological Survey's host computer operating, security, and automated job scheduling systems. Therefore, the control weaknesses increase the risk of loss of data integrity through fiscal year 1998. Accordingly, we believe that Bureau management should establish as a high priority the use of the Geological Survey's host computer systems to reduce the Bureau's risk of loss of data integrity. Additionally, management within the Bureau and the Office of the Special Trustee for American Indians did not move their applications that resided on the Center's Unisys mainframe to the Center's IBM mainframe, which would have then been moved to the Geological Survey's host computer, but instead planned to move their applications to the Unisys server. Thus the corrective actions outlined in the Bureau's response to the prior report that relied on the movement of all data processing functions from the Center to the Geological Survey were not completed.

In its response to the April 1997 audit report, the Bureau stated, "In conjunction with the transfer of mainframe data processing from the Bureau, some reorganization or redescription of positions within the Office of Information Resources Management will be necessary." The Bureau further stated that "completion of the reorganization is October 1, 1997 with an effective date of December 1, 1997." We found that Bureau management had not formally reorganized the Office of Information Resources Management but that Center management had informally reorganized the Center to prepare for providing services as a network management center. (A network management center provides enhanced customer support that uses advanced technologies for network connectivity and problem solving and developing and maintaining client/servers.*) Although the Center was being reorganized as a network management center, we did not find an approved strategic plan for such a center. As a result, corrective actions that were dependent on the reorganization of the Office of Information Resources Management were not completed.

---

[2]A "client/server" application functions on a client/server processing environment, which is a computerized architecture in which one or more "computers called servers manage shared resources and provide access to those shared resources as a service to their clients," which are personal computers. (David Vaskevitch, Client/Server Strategies. a Survival Guide for Corporate Reengineering, IDG Books Worldwide, Inc., San Mateo, California, 1993, page 96.)

Recommendation A. 1. The information technology security function be 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.

Recommendation 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- 130, Appendix III. and that Policies and procedures are implemented to keep the system security program current.

Regarding Recommendation A. 1, our prior audit found that because the Bureau's IT Security Manager function was within the Center, the security function did not have adequate independence or authority to implement and enforce a Bureauwide system security program. The security staff consisted only of the IT Security Manager and another staffperson. Most of the security staff's time was spent administering security at the Center and administering user access to the computer systems. Although users were provided written information about system security issues when access to computer systems and applications was approved, the Center did not have an employee computer security awareness training plan. Further, the security staff had not provided periodic computer security training to Bureau area and agency offices and other organizations such as schools. Additionally, a 1996 contractor-performed risk assessment recommended that the system security function be moved from the Center and elevated organizationally, but the recommendation had not been implemented at the time of our current audit.

Regarding Recommendation A.2, our prior audit found that the security implementation plan for the Bureau's automated information systems for fiscal year 1996 was not documented. Although a security implementation plan was prepared by November 1996 (for fiscal year 1997), the plan did not meet the detailed requirements of Office of Management and Budget Circular A- 130, Appendix III, "Security of Federal Automated Information Resources." The plan addressed the security needs of the Bureau, but the plan did not address the security needs of the Office of the Special Trustee or include specific steps to meet the security needs of the Bureau and the Office of the Special Trustee, thus ensuring that an adequate security program was in place for the automated systems of the Bureau and the Office of the Special Trustee. The Bureau did not have an adequate security program because the Bureau reported that "virtually no security planning" had occurred because of the downsizing of the Office of Information Resources Management. We also found that Bureau management did not assess the effectiveness of the Bureau's system security program as part of its annual review under the Federal Managers' Financial Integrity Act.

In its response to the prior audit report, the Bureau stated, as part of its reorganization and redescription of the Office of Information Resources Management, that "the position of Security Officer will be elevated to report directly to the Director of OIRM [Office of Information Resources Management]." In addition, the Bureau concurred "with respect to those functions which will remain the responsibility of the Bureau subsequent to the transfer of mainframe data processing to the U. S.G. S. [Geological Survey]" and that the development

of the policies and procedures would be the responsibility of the Bureau IT Security Manager, who would complete them by October 1, 1997. Bureau management agreed to provide the security staff with the authority to implement and enforce a Bureauwide system security program but did not agree to provide additional staff to meet the responsibilities. The Bureau stated that "[t]he recommendation would be appropriate if the Bureau were to continue to operate mainframe data processing," but that the data processing "function will be transferred to U.S.G.S. [Geological Survey], [and]. . . the Bureau Security Officer and his staff will be able to manage the reduced security requirements of the Albuquerque OIRM [Office of Information Resources Management] site."

Our followup review found that the IT Security Manager continued to report to the Acting Chief of the Center and that the IT Security Manager had not (1) developed new or revised policies and procedures for a Bureauwide system security program, (2) implemented and enforced a security program, and (3) evaluated the effectiveness of the security program. The Departmental Manual (375 DM 19) states:

> Bureau IT Security Manager is responsible for: managing the bureau IT security program, coordinating all bureau activities designed to protect IT resources, coordinating bureau IT security training programs, and reporting on the effectiveness of these activities to the bureau and Departmental management.

Additionally, Office of Management and Budget Circular A- 130, Appendix III, requires that controls over general support and major application systems be reviewed every 3 years or more frequently if significant changes are made to the systems or risks are determined to be high.[3] Further, the IT Security Manager position description included these responsibilities. However, Bureau management had not held the IT Security Manager accountable for performing these duties.

The Center was performing data processing functions and serving as a general support system, since it will continue to control the operating system, security software, and application processing for the IBM applications; operate and run a Unisys computer and applications; and operate as a network management center. We believe that the need for Bureauwide system security planning, implementation, and training and for system security oversight will not diminish but will increase and be more complex. Without a system security program, Bureau management has little assurance that its existing system security is operating effectively. Additionally, the Bureau will not be in compliance with Office of Management and Budget Circular A-l 30, Appendix III, because an adequate system security

---

[3]Office of Management and Budget Circular A- 130, Appendix III, "Security of Federal Automated Information Resources," defines a general support system as "an interconnected set of information resources under the same direct management control which shares common functionality." The Circular further states that a general support system "normally includes hardware, software, information, data, applications, communications and people" and that examples of a system are a local area network, ... an agency-wide backbone, a communications network, [and] a departmental data processing center including its operating system and utilities."

program was not in place and the system security program had not been evaluated for its effectiveness during the past 3 years. We consider these recommendations not implemented because Bureau management did not (1) elevate the IT Security Manager function to report directly to the Chief, Office of Information Resources Management; (2) hold the IT Security Manager accountable for performing position description responsibilities; and (3) ensure that the Bureau had an effective system security program. Further, we believe that once a security program is implemented, Bureau management should ensure that an evaluation of the effectiveness of the program is performed periodically and that the Bureau includes any resultant corrective actions in future Bureau security plans.

Recommendation 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.

Recommendation C. 1. The Bureau 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.

Regarding Recommendation A.3, our prior audit found that risk assessments had not been performed periodically or that they had not been performed when systems, facilities, or other conditions changed. Specifically, since 1990, only two risk assessments had been performed. These assessments were of the Center's previous mainframe configuration in 1990 and the local area networks of the Albuquerque Central Offices in 1996. While we determined that these assessments were adequate, none of the recommendations from the risk assessments had been implemented. Regarding Recommendation C. 1, we found that Bureau management had not classified its computer resources, such as data files, application programs, and computer-related facilities and equipment. Resource classification allows management to (1) determine the level of security that should be provided to protect against unauthorized modification, disclosure, loss, or impairment and (2) determine whether security controls should be implemented or document Bureau management's acceptance of the risk.

In its response to the prior audit report, the Bureau stated that "the FY [fiscal year] 1996 reduction-in-force eliminated OIRM [Office of Information Resources Management] staffs capability to perform risk assessments [and resource classifications]." The Bureau further stated that "from the resources freed as a result of the transfer of data processing and as part of the reorganization/redescription . . . , positions will be established to perform the necessary risk assessments [and resource classifications]." The Bureau also stated that the risk assessments and classifications "will commence in July 1998" and "will be completed within 18 months of that date."

We agreed with the Bureau's statement that commencement of risk assessments and resource classifications could be performed by resources that will become available as a result of transferring data processing functions to the Geological Survey. However, since the Bureau's response to the prior audit report, the then Chief, Office of Information Resources Management, retired, and the position had not been filled by the end of fiscal year 1997. Consequently, Bureau management had not developed and implemented its

reorganization/redescription for the Office of Information Resources Management. Further, we found that Center personnel had not become available to perform the assessments and classifications because the Center had not transferred all of its data processing responsibilities to the Geological Survey and was continuing to function as a general support system. In addition, Bureau management had not approved an information technology strategic plan for the Center to provide direction following the consolidation with the Geological Survey's host computer. Further, all of the owners of the Bureau's automated information system resources could not be identified. Therefore, we believe that the risk assessment and resource classification reviews cannot be performed in the time fiame identified in the Bureau's response, Accordingly, we consider these recommendations not implemented. We believe that Bureau management should redetermine when the Bureau can begin performing its risk assessments and resource classifications.

Recommendation B. 1. Ensure that personnel securitv Policies and Procedures are developed, implemented, and enforced, including those for obtaining appropriate securitv clearances for personnel in sensitive or critical ADP [automated data processing1 positions and for informing the securitv staff. in writing, whenever employees who are system users terminate their employment or are transferred.

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 emplovment has been terminated. and that verification and approval are obtained from users' supervisors and application owners or managers that the levels of access are appropriate.

Regarding Recommendation B. 1, our prior audit found that personnel in sensitive or critical ADP positions, such as system and application programmers, including application programmers not assigned to the Center, did not have documented background investigations for security clearances or did not have security clearances at a level commensurate with their positions. In addition, we found that, although the IBM computer had been set to automatically revoke a user identification (ID) after 180 days of inactivity, supervisors did not notify the application owner or manager or the Center's security staff to revoke and delete a user ID when an employee's employment was terminated or when an employee was transferred. Regarding Recommendation E. 1, we found that IT security staff and application owners did not periodically review user access authorizations to ensure that the levels of access to computer resources were appropriate.

Regarding Recommendation B. 1, the Bureau stated in its response to the prior audit report that "The necessary information will be submitted to the Office of Personnel Management to conduct/update the clearances of the Operations Service Center staff by June 1, 1997." In addition, the Bureau stated that actions will be taken to provide a report monthly to the Office of Information Resources Management which identifies employees who transferred within the Bureau and employees whose employment was terminated so that system access can be reviewed and modified or revoked.

Regarding Recommendation E. 1, the Bureau stated that the action taken to implement this recommendation was the transfer of the mainframe data processing to the Geological Survey's host computer and that December 1, 1997, was the target date for the completion of the transfer. In addition, we accepted the action to be taken by the Bureau for Recommendation B. 1, to provide a monthly report to the Office of Information Resources Management, as appropriate to partially implement Recommendation E. 1.

Our followup audit found that policies and procedures were not developed, implemented, and enforced for ensuring that (1) appropriate security clearances for personnel in sensitive or critical ADP positions were obtained, (2) security staff was informed whenever employees who were system users terminated their employment or were transferred, (3) security clearances had not been updated for all Bureau employees who filled sensitive or critical ADP positions except for 14 of the 55 Center employees who filled such positions, and (4) users' levels of access were reviewed and validated periodically. The "Generally Accepted Principles and Practices for Securing Information Technology Systems," issued by the National Institute of Standards and Technology, recommends that reviews and validation of the appropriateness of users' levels of access be performed periodically and, if necessary, the users' access be modified or revoked. Although reports were to be produced monthly that were to identify employees who had transferred within the Bureau or employees who had terminated their employment, Bureau management had not ensured that the reports were provided to the Bureau's IT security management staff. Additionally, we found that the agreement between the Bureau and the Geological Survey did not include provisions for the Geological Survey to ensure that users' levels of access were properly authorized and were appropriate for the users to perform their day-to-day duties or that access would be validated periodically for the Bureau's IBM applications.

Accordingly, we consider Recommendation B. 1 partially implemented and Recommendation E. 1 not implemented. Additionally, Bureau management should ensure that personnel who are not assigned to the Center and who are in sensitive or critical ADP positions have security clearances commensurate to the positions held. Further, if Bureau management does not require Bureau personnel to review and validate the appropriateness of users' levels of access to the Bureau's IBM applications, the agreement between the Bureau and the Geological Survey should be modified to include the requirement that the Geological Survey perform periodic reviews and validate the appropriateness of users' levels of access to the Bureau's IBM applications.

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

Recommendation D.2. Funding is provided for adequate maintenance of the commuter operations room. such as providing daily housekeeping services, or that fire-producing equipment and supplies are removed from the computer room.

Our prior audit found that the Center was located within a Federal building that provides unauthorized individuals access to the Center. To ensure that the Center and its resources were safeguarded, physical access to the Center was achieved by electronic key cards and

monitored by video cameras. However, custodial (contractor) personnel and building managers were provided key cards, which afforded an opportunity for uncontrolled access to the Center. Additionally, we found that general housekeeping and maintenance of the computer operations room were performed only weekly. This weekly schedule was not adequate because of the failure to remove potential fire hazards, such as combustible supplies and dust produced by paper used in the printer, that were housed in the computer operations room.

In its response to the prior audit report, the Bureau stated, "The action taken to implement these recommendations is the conversion of the mainframe data processing to the U.S.G.S. [Geological Survey] host computer."

Our followup audit found that, while the Bureau may no longer house the IBM and Unisys mainframe computers in the computer operations room, a clean and well-maintained computer operations room was still needed. The computer operations room housed server computers and telecommunications equipment for the Bureau's wide area network and the Albuquerque Central Office's local area networks. We found that custodial staff and building managers continued to have access to this sensitive area and that the room was cleaned only weekly. In addition, the printers and other combustible supplies remained in the room. Further, physical hazards, such as file cabinets placed in front of printers, existed for personnel who operated and maintained the computer equipment and peripherals. Therefore, we consider these recommendations not implemented.

Recommendation F. 1. Ensure that a higher priority is given to moving the applications that reside on the Unisys mainframe to the IBM mainframe.

Our prior audit found that passwords were not changed periodically and inactive user IDs were not automatically revoked on the Unisys computer. Additionally, greater reliance had to be placed on the user ID and password controls to protect the applications, files, and data because the applications residing on the Unisys computer were developed without access controls and could not be modified to install the access controls. Therefore, these controls were inadequate. However, the Bureau and the Office of the Special Trustee were planning to move the applications residing on the Unisys mainframe to the IBM mainframe.

In its response to the prior audit, the Bureau stated that it would transfer the data processing functions to the Geological Survey's host computer.

Our followup audit found that the applications which resided on the Unisys mainframe were not converted to the Bureau's IBM mainframe; therefore, the Unisys applications could not be moved to the Geological Survey's host computer. The Unisys applications could not be converted because of the lack of documented programs and because of the antiquated programming language used for the Unisys applications. The contractor estimated the cost to convert the applications to be in excess of $1 million. However, as an interim solution, the Department's Office of Information Resources Management approved the Bureau's acquisition of a Unisys server computer. The applications would be moved from the Unisys mainframe to the Unisys server. The Department's Office of Information Resources

Management stated that the Bureau should continue to convert these applications to operate on an IBM mainframe computer. In our opinion, because the Office of the Special Trustee was redeveloping its applications that reside on the Unisys server computer, the Unisys applications should not be converted to the Geological Survey's host computer, as originally recommended, but be maintained on the Unisys server until the Office of the Special Trustee's redevelopment project is completed. This action could save the Bureau at least $1 million in conversion costs. We believe that the Bureau should not implement the original recommendation because of the costs involved in converting the Unisys applications. Accordingly, we consider the recommendation resolved because it is no longer applicable.

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.

Our prior audit found that the software development and change controls were inadequate to ensure that the proper version of an application was used in production. Based on our test of the National Irrigation Information Management System, we found that the application programmers 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, the lead programmer was not notified of software modifications. Further, one member of the Center's systems staff, who was a programmer, could move application software changes from test or development into production without the approval of the lead programmer.

In its response to the prior report, the Bureau stated that the Office of Information Resources Management was "in the process of expanding and documenting improved procedures in this area" and that the target date for completion was July 1, 1997.

Our followup audit found that new or revised policies and procedures related to application development and changes were not developed and that individuals had not been assigned responsibilities for application development or changes. Because the policies and procedures had not been developed and responsibility had not been assigned, controls for application software development and change had not improved. For the National Irrigation Information Management System, the application programmers continued to test applications and to approve the movement of the modified programs into production without the knowledge of the lead programmer. For the Loan Management and Accounting System, the application developer did not fully document change requests or modifications to the System. In addition, the Loan Management and Accounting System application developer had full access to user passwords and the loan databases. Further, Center personnel and contractors were developing client/server applications without any documented Bureau management support. Accordingly, we consider this recommendation not implemented.

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

Recommendation I. 1. Ensure that access and activities of the Center's system programmers are controlled and monitored bv security staff and that Resource Access Control Facility (RACF) controls are established to Protect system resources.[4]

Regarding Recommendation H.1, our prior audit found that the duties for the support functions of system design, application programming, systems programming, quality assurance/testing, library management, change management, data control, data security, and data administration were not adequately segregated between different individuals.

Regarding Recommendation I. 1, we found that controls established over system software were not effective in detecting and deterring inappropriate use. Specifically, periodic reviews of the System Maintenance Facility logs and RACF access reports were not performed by the security staff to monitor system activities effectively. Additionally, the security staff produced reports that identified users and the computer resources accessed; however, the staff had not produced or used the primary "auditing" or monitoring reports that could be used to provide oversight of system activities. One system programmer had "alter" access to system software, the System Maintenance Facility logs, and RACF logs, which provided an opportunity for the programmer to alter his activities, as well as those of other users. Thus, the audit trails of system activities could be impaired or destroyed. Further, the RACF could be used to establish controls and monitor access to the computer resources, but it had not been set up to effectively control access to the system resources. We found that one of the "start procedures" could bypass all verification processing, including the security classification checks, and therefore affect the overall security of the system. Further, RACF was not used to protect critical system resources, including the system parameter library, linklist libraries, master catalog, and the primary and backup files. Finally, no logging or audit trails were available.

In its response to the prior audit report, the Bureau stated that it will implement these recommendations through the "conversion of the mainframe data processing" to the Geological Survey's host computer.

Our followup audit found that Center management had not segregated system functions and had not changed the use of the RACF to be an effective critical resource control. Specifically, functions such as systems design, application programming, systems programming, quality assurance/testing, library management, change management, data control, data security, and data administration had not been segregated between different individuals. Further, one system programmer continued to have "alter" access to system software, the System Maintenance Facility logs, and RACF logs. Because the Center will continue to maintain control over the IBM operating system and security software at the Geological Survey's host computer through at least fiscal year 1998 and will continue to

[4]Resource Access Control Facility (RACF) is an IBM-licensed software security product that protects information by controlling access to the information. RACF provides security by identifying and verifying users to the system, authorizing users' access to protected resources, and recording and reporting access attempts. (Resource Access Control Facility General Users Guide, Version 1. Release 9.2, 9th edition, IBM Corp., 1993, page l-l.)

operate Unisys applications, the need for segregation of duties between different individuals and the use of RACF controls to protect system resources still exists. Accordingly, we consider these recommendations not implemented.

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.

Our prior audit found that the Center did not have an effective means to recover or to resume computer operations in the event of a system failure or a disaster. The Center was developing a service continuity plan for fiscal year 1997. The off-site storage facility was not located at least 1 mile from the Center, and the facility did not adequately safeguard information and data stored from unauthorized access and environmental hazards such as heat and humidity. Thus, the data stored were at risk of loss or damage.

In its response to the prior audit report, the Bureau stated, "To ensure service continuity in case of system failure or a disaster, the Office of Information Resources Management (OIRM) has a contract for back-up of it's a-17 [Unisys] computer." The Bureau further stated, "OIRM has determined that a similar contract for its IBM 3090 computer is not warranted because of the pending transfer to the U.S. Geological Survey (USGS) of the data processing operation." The Geological Survey had indicated that it had a contract which would cover the Bureau's systems during the transfer to the host computer. The Bureau did not specifically respond to the recommendation on acquiring a secure off-site storage facility.

Our followup audit found that the Bureau did have a contract and, in a test situation, had successfully recovered its Unisys applications. However, the Bureau had not acquired an environmentally sound and secure off-site storage location. As such, the backup tapes were stored on-site in the Center's computer room. Accordingly, we consider the recommendation partially implemented.

## Recommendations

We recommend that the Assistant Secretary for Indian Affairs ensure that the Bureau of Indian Affairs:

1. Establishes as a high priority the use of the Geological Survey's host computer's operating, security, and automated job scheduling systems.

2. Develops and approves an Office of Information Resources Management strategic plan which provides direction to and defines the functions of the Operations Service Center.

3. Holds the IT Security Manager accountable for performing the position responsibilities.

4. Performs periodically an evaluation of the system security program's effectiveness and includes any resultant corrective actions in future Bureau security plans.

5. Redetermines, 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.

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

7. Requires 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 be performed for the IBM applications by the Geological Survey.

8. Removes all safety hazards from the computer operations room.

## Bureau of Indian Affairs Response and Office of Inspector General Reply

In the May 19, 1998, response (Appendix 2) from the Assistant Secretary for Indian Affairs to this audit report, the Bureau concurred with Recommendations 1, 2, 3, 4, 5, 6, and 7 and concurred "in part" with Recommendation 8. Based on the response, we consider Recommendations 1 and 8 resolved and implemented and Recommendations 2, 3, 4, 5, and 6 resolved but not implemented. Accordingly, the unimplemented recommendations will be referred to the Assistant Secretary for Policy, Management and Budget for tracking of implementation. Also based on the response, the Bureau is requested to provide additional information for Recommendation 7 (see Appendix 3).

Regarding our April 1997 report, the Bureau in its May 1998 response, concurred with Recommendations A. 1, A.2, A.3, B. 1, C. 1, E. 1, G. 1, H. 1, I. 1, and J. 1 and concurred in part with Recommendations D. 1 and D.2. Based on the response, we consider Recommendations A. 1, D. 1, I. 1, and J. 1 resolved and implemented and Recommendations A.2, A.3, B. 1, C. 1, D. 1, E. 1, G. 1, and H. 1 resolved but not implemented (see Appendix 4). Accordingly, this information on the prior recommendations will be forwarded to the Assistant Secretary for Policy, Management and Budget.

In accordance with the Departmental Manual (360 DM 5.3), we are requesting a written response to this report by July 10, 1998. The response should provide the information requested in Appendix 3.

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"

| 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. | Not implemented. Bureau management had not reorganized the Office of Information Resources Management to elevate the information technology security function to report directly to the Director, Office of Information Resources Management. Bureau management also had not ensured that the information technology security function was provided with authority to implement and enforce a Bureauwide system security program. In its response, Bureau officials stated that the staff would not be increased because of the transfer of data processing functions to the Geological Survey, which has not occurred. |
| 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, and that policies and procedures are implemented to keep the system security program current. | Not implemented. A revised system security program and new or revised policies and procedures had not been developed, and an evaluation of the security program's effectiveness had not been performed. |
| 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. Corrective actions to implement the recommendation, such as the reorganization of the Office of Information Resources Management and the transfer of data processing functions to the Geological Survey, had not occurred. |

| | |
|---|---|
| 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 ADP positions and for informing the security staff, in writing, whenever employees who are system users terminate their employment or are transferred. | Partially implemented. No new or revised personnel security policies and procedures had been developed. Although the necessary paperwork to initiate security clearances for 14 Center employees had been prepared, security clearance paperwork had not been initiated for employees who were not assigned to the Center and performed ADP sensitive and critical functions. Also, Bureau management was to provide the security staff with monthly reports that identified Bureau personnel who had terminated their employment or who were transferred; however, the reports had not been provided to the security staff. |
| 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. No new or revised policies had been developed. Additionally, Bureau management had not taken corrective actions, such as reorganizing the Office of Information Resources Management and transferring data processing functions. |
| D. 1. Sufficient staff are provided to adequately monitor all visitor activities. | Not implemented. Corrective actions were dependent upon transferring data processing functions to the Geological Survey, which had not occurred. However, the Center had installed server computers and network communications equipment that also required safeguarding. |
| D.2. Funding is provided for adequate maintenance of the computer operating room, such as providing daily housekeeping services, or that fire-producing equipment and supplies are removed from the computer room. | Not implemented. Corrective actions were dependent upon data processing functions being transferred to the Geological Survey, which had not occurred. However, the Center had installed server computers and telecommunications equipment in the computer operations room, which also needed to be protected from dust and fire hazards. |

| | |
|---|---|
| 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 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. No new or revised policies had been developed. Additionally, Bureau management was to provide the security staff with monthly reports identifying Bureau personnel who had terminated their employment or who were transferred; however, the reports had not been provided to the security staff. Additionally, Bureau management's corrective action was dependent upon transferring data processing functions to the Geological Survey. However, data processing functions were not transferred, and the agreement between the Bureau and the Geological Survey did not contain provisions for the Geological Survey to ensure that users' levels of access were properly authorized and were appropriate for the users to perform their day-to-day duties or that the access would be validated periodically. |
| F. 1. Ensure that a higher priority is given to moving the applications that reside on the Unisys mainframe to the IBM mainframe. | Resolved. The recommendation is no longer applicable. |
| 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. No new or revised policies had 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. | Not implemented. Corrective actions were dependent upon data processing functions being transferred to the Geological Survey. However, for at least fiscal year 1998, the Bureau will continue to operate and control the IBM operating system and security software after the transfer to the Geological Survey. Additionally, the Bureau will be operating and controlling a Unisys server computer and maintaining the applications that will reside on the Unisys computer. |
| I. 1. Ensure that access and activities of the Center's system programmer are controlled and monitored by security staff and that RACF controls are established to protect system resources. | Not implemented. Corrective actions were dependent upon data processing functions being transferred to the Geological Survey. However, for at least fiscal year 1998, the Bureau will continue to operate and control the IBM operating system and security software. |
| 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. Although a contingency plan had not been developed, the Bureau had contracted for a backup site for the Unisys mainframe computer in the event of a disaster and had tested the functionality of the backup site. Additionally, the Geological Survey had agreed to include the Bureau's operating system and security and application software as part of the Geological Survey's contingency plan. However, Bureau management had not acquired a secure off-site storage facility for the data and files. |

# United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, D.C. 20240

MAY 19 1998

Memorandum

**To:** Assistant Inspector General for Audits

From: Assistant Secretary - Indian Affairs

Subject: Draft Audit Report on Followup of General Controls Over Automated Information Systems, Operations Service Center, Bureau of Indian Affairs (A-IN-BIA-00 1-97)

The subject audit report addresses the Bureau of Indian Affairs (Bureau) implementation of the recommendations made by the Office of Inspector General in its April 1997 audit report entitled "General Controls Over Automated Information Systems_ Operations Service Center, Bureau of Indian Affairs" (Report No. 97-I-771). The followup audit found that the Bureau had partially implemented 2 of the 13 recommendations made in the April 1997 report and had not implemented 10 recommendations and that 1 recommendation was no longer applicable. The audit concluded that the general control risks identified by the prior audit for fiscal year 1996 continued to exist during fiscal year 1997. The subject audit report includes eight new recommendations.

The Bureau generally agrees with the findings of the followup audit. As noted in our response to the April 1997 audit, the Office of Information Resources Management was to undergo a reorganization and redescription of positions because of the transfer of mainframe data processing from the Bureau to the U.S. Geological Survey. Although the reorganization/ redescription began in fiscal year 1997, the resignation of the Director and the transfer and subsequent retirement of the Deputy Director limited its effectiveness. The reorganization is well underway, and the Acting Director, Office of Information Resources Management is on-site in Albuquerque, New Mexico. As discussed below, the Service Center has taken actions to implement many of the recommendations and to improve its controls. Finally, the Bureau appreciates the changes made to the draft report from our discussions on the preliminary draft report.

As requested, we have provided a revised corrective action plan for the unimplemented recommendations. To avoid repeating corrective actions, we have included the new recommendations with the unimplemented recommendations from the prior audit.

**Followup Audit Recommendation 1.** We recommend that the Assistant Secretary - Indian Affairs ensure that the Bureau of Indian Affairs establishes as a high priority the use of the Geological Survey's host computer's operating, security, and automated job scheduling functions.

**Bureau Response.** The Bureau concurs. The Service Center will complete the transfer of all IBM mainframe operations, system software support, and security administration functions to the U.S. Geological Survey Data Center in Reston, Virginia. by May 3 1, 1998. We consider this recommendation implemented.

**Followup Audit Recommendation 2.** We recommend that the Assistant Secretary - Indian Affairs ensure that the Bureau of Indian Affairs develops and approves an Office of Information Resources Management strategic plan which provides direction to and defines the functions of the Operations Service Center.

**Bureau Response.** The Bureau concurs. A comprehensive strategic plan for the Office of Information Resources Management is being developed and finalized under contract with MitreTek. The strategic plan will be completed by September 30, 1998. The responsible official is the Director, Office of Information Resources Management.

**Prior Audit Recommendation A.1.** The information technology security function be 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.

**Followup Audit Recommendation 3.** We recommend that the Assistant Secretary - Indian Affairs ensure that the Bureau of Indian Affairs holds the IT Security Manager accountable for performing the position responsibilities.

**Bureau Response. The** Bureau concurs. The Information Technology Security Manager's position has reported to the Office Director since October 1997. (See Attachment 1.) The position has Bureauwide authority for the information technology security program. As noted in our response to the prior report, we believe that sufficient staff will be available to manage the security requirements once we transfer the remaining processing functions for the IBM computer to the Geological Survey. As with all employees, Bureau management will hold the Security Manager accountable through the performance appraisal process. The reorganization will be completed by September 30, 1998. The responsible official is the Director, Office of Information Resources Management.

**Prior Audit Recommendation 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-130, Appendix III, and that policies and procedures are implemented to keep the system security program current.

**Followup Audit Recommendation 4.** We recommend that the Assistant Secretary - Indian Affairs ensure that the Bureau of Indian Affairs performs periodically an evaluation of the system security program's effectiveness and includes any resultant corrective actions in future Bureau security plans.

**Bureau Response.** The Bureau concurs. The Bureau has entered into an agreement with Washington Administrative Service Center- West to develop a comprehensive computer security plan

that will address computer security policies, operating procedures, responsibilities, contingency planning and risk analysis. (See Attachment 2.) The plan will be developed in accordance with the standards and guidance published in the Office of Management and Budget Circular A-130; the National Institute of Standards and Technology's Federal Information Processing Standards Publications dealing with automated information system security; and the Office of Personnel Management's Federal Personnel Manual issuances on personal security as they relate to automated information systems. The plan's operating procedures and the management control reviews required by the Department's Office of Information Management will ensure that the plan be periodically reviewed and updated. The plan will be developed by July 3 1, 1998. The responsible official is the Information Technology Security Manager.

**Prior Audit Recommendation 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.

**Prior Audit Recommendation C.l.** 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.

**Followup Audit Recommendation 5.** We recommend that the Assistant Secretary - Indian Affairs ensure that the Bureau of Indian Affairs redetermines, 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 risk assessments resource classifications should be identified.

**Bureau Response.** The Bureau concurs. Risk assessments and classifications of the Bureau's automated information systems environment will be performed beginning in fiscal year 1999 in accordance with the Bureau's security program plan. The Information Technology Security Management staff will provide oversight of this effort. Risk assessments and classifications will be done by teams consisting of personnel from the Bureau's Office of Information Resources Management and the program offices.

**Prior Audit Recommendation 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 ADP positions and for informing the security staff, in writing, whenever employees who are system users terminate their employment or are transferred.

**Prior Audit Recommendation E.l.** Ensure that policies are developed and implemented which match personnel files with system users periodically, that user ID(s) 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.

**Followup Audit Recommendation 6.** We recommend that the Assistant Secretary - Indian Affairs ensure that the Bureau of Indian Affairs obtains security clearances for ADP personnel who are not assigned to the Center that are commensurate with their positions.

**Followup Audit Recommendation 7.** We recommend that the Assistant Secretary - Indian Affairs ensure that the Bureau of Indian Affairs requires 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 be performed for the IBM applications by the Geological Survey.

**Bureau Response.** The Bureau concurs. In February 1998, the Bureau reorganized its position sensitivity and security program. As part of this effort, the Central Office is reviewing all sensitive positions, including information technology positions, to determine whether the positions are classified consistently. Once the position descriptions are reviewed, the personnel system will be updated and a listing generated that will identity individuals needing initial and upgraded investigations or reinvestigations. While we will complete this initial effort by September 30, 1998, the scheduling of the investigations will be dependent on available area office funding. The Bureau's Security Officer, however, will monitor the area offices to ensure that the investigations are completed. In addition, the Information Technology Security Manager will ensure that the employee termination report is received and reconciled with system users. The report will also be provided to the Geological Survey for its use in managing Bureau system user profiles.

**Prior Audit Recommendation D.l.** Sufficient staff are provided to adequately monitor all visitor activities.

**Prior Audit Recommendation D.2.** Funding is provided for adequate maintenance of the computer operating room, such as providing daily housekeeping services, or that fire-producing equipment and supplies are removed from the computer room.

**Followup Audit Recommendation 8.** We recommend that the Assistant Secretary - Indian Affairs ensure that the Bureau of Indian Affairs removes all safety hazards from the computer room.

**Bureau Response.** The Bureau concurs in part. We believe that we have implemented these recommendations to the extent possible given our available resources. Monitoring of visitor activities is handled by the organizational element receiving the visitor(s). All non-Service Center personnel must register with the Information Technology Security Manager. A minimum number of access keys have been provided to custodial, building security, and GSA building managers based upon their need to enter the facility. In addition, the Service Center has funded full time housekeeping and maintenance service for the computer room and ancillary facilities beginning in fiscal year 1998. Finally, the Service Center has corrected the safety deficiencies identified by the Division of Safety Management in its annual safety and health evaluation for fiscal year **1997.**

**Prior Audit 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.

**Bureau Response.** The Bureau concurs. The Bureau recruited and filled the Chief, Applications Support Branch, position in November 1997. The Branch is developing and implementing standards,

procedures, and policies to ensure full accountability for all application system change management and production implementation of the Office's applications. This guidance, when finalized, will be distributed to all Bureau offices which develop and/or maintain application systems. The responsible official is the Chief, Applications Support Branch.

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

**Prior Audit Recommendation 1.1.** Ensure that access and activities of the Center's system programers are controlled and monitored by security staff and that Resource Access Control Facility (RACF) controls are established to protect system resources.

**Bureau Response.** The Bureau concurs. This has been accomplished for the applications residing on the IBM computer with the transfer of the remaining application operations system software support, and security functions to the Geological Survey. The operating system and security features of the new Unisys NX Server provide much improved safeguards for the data and applications residing on this platform. Although RACF controls are not compatible with the Unisys NX Server, the Bureau will establish similar controls. Finally, separation of duties, to the extent possible, was considered during the reorganization/redescription of positions for the Service Center. We consider these recommendations implemented.

**Prior Audit 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.

**Bureau Response.** The Bureau concurs. As stated in the draft audit report, the Bureau has a disaster recovery contract that has been fully tested and certified for the Unisys hosted applications. In addition, the Bureau has obtained off-site storage for its backup media at the Southwestern Indian Polytechnic Institute which is approximately 8 miles from the Service Center. We consider this recommendation implemented.

Attachments

IN REPLY REFER TO:

# United States Department of the Interior

BUREAU OF INDIAN AFFAIRS
Information Resources Management
Operations Service Center
500 Gold Avenue, S.W.
P.O. Box 888
Albuquerque, New Mexico 87103

Office of Information Resources Management
Operations Service Center
MS-611

FEB - 3 1998

MEMORANDUM

REPLY TO
ATTN OF: Acting Director, Office of Information Resources Management

SUBJECT: Bureau AIS Security Officer Status.

TO: Acting Director, Management and Administration

In accordance with the recommendation of the Department Inspector General, Position Number K00283-01223, GS-0334-13, Computer Specialist within our Operations Service Center, has reported directly to the undersigned since October 26, 1997.

This position is encumbered by Jerry K. Belew, who is currently designated the BIA Automated Information Systems (AIS) Security Administrator.

George Gover
Acting Director, OIRM

*CC:*
Personnel office, Albuquerque Area Office
Jerry Fiely, Deputy Director - Audit & Evaluation

*WASC-West Project Scope Statement*
*March* 1998
*Revised March 10,* 1998

**Project Number 98-053**

**Project Title**
Development of Security Plan

**Client**
BIA

**Program Manager**
Tony Manzi, WASC-West

**Project Leader**
Ellen Erikson

**Project Team**
WASC: Jim Opeka
USGS: Blanche Heard
BIA: Jerry Belew; Lorraine Jaramillo; Wesley Anderson

**Project Description**

**Problem Statement**
The Bureau of Indian Affairs (BIA) has identified the need to develop a comprehensive computer security plan. The plan will address computer security policies, operating procedures, responsibilities, contingency planning, and risk analysis. The plan should be developed in accordance with the standards and guidance published in the Office of Management and Budget (OMB) Circular No. A-130; the National Institute of Standards and Technology's Federal Information Processing Standards Publications (FIPS PUBS) dealing with automated information system security; and the Office of Personnel Management's Federal Personnel Manual issuances on personal security as they relate to automated information systems.

**Background**
BIA recently transferred its mainframe computer applications from Albuquerque, NM to the U.S. Geological Survey (USGS) mainframe computer in Reston, VA The applications are currently operating in a separate partition of the USGS mainframe. BIA is responsible for administering security for these applications. There are still a number of BIA applications running on hardware located in Albuquerque, NM. BIA staff is also responsible for security at the Albuquerque installation.

In addition, the Office of the Inspector General issued a draft audit report (A-IN-BIA-

001-97) in February 1998, that identifies a number of issues and recommendations relative to computer security.

The proposed security plan needs to address security policies, standards, and procedures that are applicable to the current operating environment, consistent with applicable USGS policies and procedures, and responsive to the recommendations in the draft audit report.

**Project Objectives**

**The** objective of this project is to develop a comprehensive computer security program that:

- complies with applicable Federal regulations and guidelines,
- provides an appropriate response to the OIG draft audit report, and
- ensures that BIA hardware, software, and application data is secure.

The computer security program will address the following:

- security policies, standards, and operating procedures,
- administrative, physical, application., and personal security,
- individual and organizational security responsibilities,
- contingency and disaster recovery planning,
- risk analysis policies and procedures.

**Target Deliverable Dates**

| | |
|---|---|
| March 20, 1998 | Proposed Project Scope Statement delivered to BIA |
| April 3, 1998 | Proposed Project Scope Statement approved by BIA |
| April 10, 1998 | Detailed project plan delivered to BIA |
| May 29, 1998 | Draft security plan delivered to BIA |
| June 19, 1998 | Draft security plan approved by BIA |
| July 3, 1998 | Fii security plan delivered to BIA |
| July 10, 1998 | Proposal for implementing security plan delivered to BIA (if requested) |

## Project Methodology

**General Approach**

A project team will be established that includes representation from BIA, the WASC, and USGS. The team will review appropriate Federal guidelines and regulations, interview applicable computer personnel, inventory BIA applications residing in Reston and Albuquerque, review applicable USGS computer security plans, and review the OIG draft report findings and recommendations. The project leader will provide periodic project status updates to the WASC-West program manager who in turn will provide updates to

BIA management. Policy and procedures issues will be brought to BIA management for resolution as required.

**Assumptions**

BIA applications currently operating in a separate partition of the USGS mainframe computer will eventually migrate to the general production area of the mainframe and RACF security for BIA will be integrated into the regular production RACF security database.

Mainframe computer security administration will eventually be the responsibility of USGS personnel.

At least one member of the project team will be familiar with the BIA Unisys system applications and access controls.

# STATUS OF CURRENT AUDIT REPORT RECOMMENDATIONS

| Finding/Recommendation Reference | status | Action Required |
|---|---|---|
| land8 | Implemented. | No further action is required. |
| 2, 3, 4, 5, and 6 | Resolved; not implemented. | No further response to the Office of Inspector General is required. The recommendations will be referred to the Assistant Secretary for Policy, Management and Budget for tracking of implementation. |
| 7 | Management concurs; additional information needed. | Provide target dates for when (1) the IT Security Manager will begin receiving the employee termination reports and (2) the supervisors and application owners will begin approving levels of access. Additionally, a copy of the modified agreement with the Geological Survey requiring access reviews and verifications should be provided to the Office of Inspector General. |

# STATUS OF PRIOR AUDIT REPORT RECOMMENDATIONS

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

# ILLEGAL OR WASTEFUL ACTMTIES SHOULD BE REPORTED TO THE OFFICE OF INSPECTOR GENERAL BY:

Sending written documents to:

Calling:

## 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 22201

(703) 235-9221

### North Pacific Region

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

(67 1) 647-605 1

**Toll** Free **Numbers:**
I-800-424-5081
**TDD** I-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