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

AUDIT REPORT

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

REPORT NO. 97-I-771
APRIL 1997

United States Department of the Interior

OFFICE OF INSPECTOR GENERAL
Washington, D.C. 20240

MAY 12 1997

MEMORANDUM

TO: The Secretary

FROM: Wilma A. Lewis
Inspector General

SUBJECT SUMMARY: Final Audit Report for Your Information - "General Controls Over Automated Information Systems, Operations Service Center, Bureau of Indian Affairs" (No. 97-I-771)

Attached for your information is a copy of the subject final audit report. The objective of our audit was to evaluate the adequacy of general controls over automated information systems at the Bureau of Indian Affairs Operations Service Center.

We found that the Bureau's general controls over its automated information systems at the Center were not effective. Specifically, the Bureau did not: have an effective system security program and had not enforced personnel policies and procedures to ensure adequate system security; classify its resources to determine the level of security necessary; monitor visitor activities and perform adequate housekeeping to safeguard the mainframe computers and other peripheral devices and media; perform periodic reviews to ensure that users' access levels to the mainframe computers were appropriate; ensure that the proper version of an application was used in production; have segregation of duties for the systems support functions; have controls over system software to effectively detect and deter inappropriate use; and have an effective means of recovering or of continuing computer operations in the event of a system failure. We made 14 recommendations to improve management and internal controls over the Bureau's automated information systems at the Center.

The Bureau concurred with 12 of the 14 recommendations, disagreed with 1 recommendation, and did not address 1 recommendation. Based on the response from the Acting Assistant Secretary for Indian Affairs, we considered 12 recommendations resolved but not implemented and two recommendations unresolved. We revised one of the unresolved recommendations and requested that the Bureau provide additional information on the remaining recommendation, which the Acting Assistant Secretary had not addressed.

If you have any questions concerning this matter, please contact me at (202) 208-5745 or Mr. Robert J. Williams, Assistant Inspector General for Audits, at (202) 208-4252.

Attachment

United States Department of the Interior

OFFICE OF INSPECTOR GENERAL
Washington, D.C. 20240

APR 3 0 1997

AUDIT REPORT

Memorandum

To: Assistant Secretary for Indian Affairs

From: Robert J. Williams
Assistant Inspector General for Audits

Subject: Audit Report on General Controls Over Automated Information Systems, Operations Service Center, Bureau of Indian Affairs (No. 97-I-771)

INTRODUCTION

This report presents the results of our audit of general controls over automated information systems at the Bureau of Indian Affairs Operations Service Center. The objective of our audit was to evaluate the adequacy of general controls over the Center's mainframe computer systems and its processing environment in the areas of security program development, access, software development and change management, segregation of duties, system software, and service continuity.

BACKGROUND

The Bureau's Operations Service Center is organizationally under the Bureau's Office of Information Resources Management and is located in Albuquerque, New Mexico. The Center provides computer services such as telecommunications, running applications, systems recovery, and user support and is responsible for the Bureau's automated information systems security. The Center operates all of the Bureau's major and sensitive mainframe applications (except for the Federal Financial System), such as the Land Records Information System and the National Irrigation Information Management System, on an IBM mainframe computer. The Center also operates major and sensitive mainframe applications of the Office of the Special Trustee for American Indians, such as the Individual Indian Monies System, on a UNISYS mainframe computer. The Center processes approximately 2.5 million transactions weekly.

The IBM computer is used as a link between many of the area and agency offices and the Bureau's Federal Financial System, located in Reston, Virginia, and as a link to many of the

applications residing on the UNISYS computer. However, during our review, the Bureau and the Office of the Special Trustee were moving the applications that reside on the UNISYS computer to the IBM computer.

SCOPE OF AUDIT

We reviewed the Bureau's general controls that were in place for its automated information systems. Specifically, we reviewed the general controls at the Operations Service Center and general controls, such as Bureau policies, that affected the Center's operations during fiscal year 1996 and for the two months of fiscal year 1997 (through November 1996). We reviewed the controls for security program development, access, software development and change control, segregation of duties, system software, and service continuity as they related to the two mainframe computers and to Center operations. However, we did not review the controls related to the UNISYS computer for software development and change management and system software because the UNISYS computer applications were being moved to operate on the IBM computer. To accomplish our objective, we reviewed the Bureau's automated information system security program, interviewed Center personnel and application owners and managers, reviewed systems documentation, observed and became familiar with Center operations, and analyzed system security.

Our audit, which was conducted during August through December 1996, was made in accordance with the "Government Auditing Standards," issued by the Comptroller General of the United States. Accordingly, we included such tests of records and other auditing procedures that were considered necessary under the circumstances,

As part of our review, we evaluated the internal controls that could adversely affect the Center's data processing environment. The control weaknesses that we found are discussed in the Results of Audit section of this report, If implemented, the recommendations should improve the general controls.

PRIOR AUDIT COVERAGE

During the past 5 years, the General Accounting Office has not issued any reports related to the Bureau's automated information systems. However, in December 1996, the Office of Inspector General issued the audit report "Statement of Assets and Trust Fund Balances at September 30, 1995, of the Trust Funds Managed by the Office of Trust Funds Management, Bureau of Indian Affairs" (No. 97-I-96) which presented the results of an audit of the Trust Funds conducted by an independent public auditor. The independent public auditor reported that material internal control weaknesses existed in computerized systems. Specifically, the independent public auditor reported that: (1) the physical location of the two mainframes is a "high risk location" and that only "informal arrangements" have been made with other Governmental agencies to provide recovery services in the event of a disaster; (2) security controls over the UNISYS mainframe computer were "inadequate" because "the system does

not require automatic password changes periodically, users are not automatically logged out after a specified period of inactivity, and there is no limit to the number of invalid password attempts made by a user"; and (3) "changes to the Individual Indian Monies (IIM) application are not performed in a test environment on the UNISYS mainframe" and "there are no procedures in place for subsequent review after changes have been implemented." The report contained recommendations for the Office of the Special Trustee for American Indians to correct these deficiencies. In its response, the Office said that these areas were the responsibility of the Bureau of Indian Affairs and that it had provided, for the Deputy Commissioner of Indian Affairs consideration, a copy of the Internal Control Report which made these recommendations. However, the Bureau was not provided an opportunity to respond to the report. We found that the deficiencies relating to the scope of our current audit (the location of the two mainframe computers, recovery services, and security controls over the UNISYS computer) still existed, as discussed in the Results of Audit section of this report.

RESULTS OF AUDIT

We concluded that the Bureau of Indian Affairs general controls over its automated information systems at the Operations Service 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. Office of Management and Budget Circular A-130, "Management of Federal Information Systems," and National Institute of Standards and Technology Federal Information Processing Standards Publications require Federal agencies to establish and implement computer security and management and internal controls to protect sensitive information in the computer systems of executive branch agencies.[1] Additionally, the Congress enacted laws, such as the Privacy Act of 1974 and the Computer Security Act of 1987, to improve the security and privacy of sensitive information in computer systems by requiring executive branch agencies to ensure that the level of computer security and controls is adequate. However, the Bureau had not complied with the criteria in that it had not developed a formal, up-to-date, comprehensive system security program or established formal policies, standards, and procedures for computer operations. Additionally, the security officer function was not at the appropriate organizational level, and adequate funding and personnel were not provided to fully support the Center's mission. 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 the 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.

[1]The Computer Security Act of 1987 defines sensitive data as "any information the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act."

Overall, we identified 10 weaknesses and made 14 recommendations for improving management and internal controls for the Bureau's automated information systems at the Center. The weaknesses within the six major areas of system security, access, software development and change controls, segregation of duties, system software, and service continuity are provided in the following paragraphs, and specific details of the weaknesses and our respective recommendations to correct these weaknesses are in Appendix 1.

System Security Program

We found that the Bureau did not have an effective system security program and had not enforced personnel policies and procedures to ensure adequate system security. As a result, the Bureau increased the risk that mission-based, sensitive computer systems are not adequately protected and that sensitive data may be impaired or compromised by individuals, including individuals whose employment has been terminated or who have been transferred. We made five recommendations to address these weaknesses.

Access Controls

We found weaknesses in physical and logical access controls over the mainframe computers.[2] Specifically, the Bureau did not classify its resources to determine the level of security necessary; monitor visitor activities and perform housekeeping functions periodically to safeguard the mainframe computers, local area network (LAN) equipment, and daily backup tape libraries at the Center; perform periodic reviews to ensure that users' access levels to the mainframe computers were appropriate; and change passwords periodically for access to the UNISYS computer. As a result, the Bureau increased the risk of unauthorized access and damage to and the destruction of mainframe computer hardware, software, and data. We made five recommendations to address these weaknesses.

Software Development and Change Controls

We found that software development and change controls were inadequate to ensure that the proper version of an application was used in production. As a result, the Bureau increased the risk of (1) security features being inadvertently or intentionally omitted or turned off and (2) irregularities or "malicious codes" being introduced.[3] We made one recommendation to address this weakness.

---

[2]Logical access involves the use of computer hardware and software to prevent or detect unauthorized access by requiring users to input user identifications, passwords, or other identifiers that are linked to predetermined access privileges.

[3]The National Institute of Standards and Technology's handbook, "An Introduction to Computer Security: The NIST Handbook," defines "malicious codes" as "viruses, worms, Trojan horses, logic bombs, and other 'uninvited software."

Segregation of Duties

We found that there was inadequate segregation of duties for the systems support functions in the areas of system design, application programming, systems programming, quality assurance/testing, library management, change management, data control, data security, and data administration. As a result, the Bureau increased the risk of (1) implementing improper program changes and (2) damaging or destroying computer resources. We made one recommendation to address this weakness.

System Software

We found that the controls established over system software were not effective in detecting and deterring inappropriate use. Specifically, periodic reviews of the System Maintenance Facility logs and Resource Access Control Facility (RACF) reports were not performed, access to the logs and to the RACF reports was not adequately controlled, and the RACF had not been set up effectively. As a result, the Center increased the risk of not detecting alterations through normal operating controls, We made one recommendation to address this weakness.

Service Continuity

We found that the Center did not have an effective means of recovering or of continuing computer operations in the event of a system failure or a disaster. Specifically, the Center did not have a service continuity plan, and the off-site storage facility, which houses backup information such as software applications, databases, and data, was not located at least 1 mile away from the Center, was not secure, and was not environmentally protected. As a result, the Center may not be able to recover or resume critical computer operations in the event of a system failure or a disaster. We made one recommendation to address this weakness.

Bureau of Indian Affairs Response and Office of Inspector General Reply

In the March 19, 1997, response (Appendix 2) from the Acting Assistant Secretary for Indian Affairs to the draft report, the Bureau concurred with 12 of the draft report's 14 recommendations, disagreed with 1 recommendation, and did not specifically address 1 recommendation.

In its response to Recommendation A.2 in our draft report, the Bureau stated that the recommendation "would be appropriate" if the Bureau were to continue to operate mainframe data processing." The Bureau further stated, "Since that function will be transferred to U.S.G.S. [U.S. Geological Survey], we believe that 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." We agree that if the Bureau transfers the data processing function to the U.S. Geological Survey, the recommendation is not needed.

Therefore, we have eliminated Recommendation A.2 from the final report and have renumbered Recommendations A.3 and A.4 from our draft report accordingly. However, a separate security function would be required at the Center should data be processed by the Center after mainframe data processing ceases.

Regarding Bureau plans for automated information systems, the Bureau stated that, because of the transfer of mainframe data processing from the Bureau to the U.S. Geological Survey beginning in July 1997, the Office of Information Resources Management will be reorganized or positions will be redefined by October 1, 1997, and implemented by December 1, 1997. Because of the transfer of mainframe data processing, according to the Bureau, recommendations applicable to physical controls, user access, access to the UNISYS computer, segregation of duties, and systems software will be implemented through the actions taken as part of the conversion. The Bureau further stated that the information systems security position "will be elevated to report directly" to the Director, Office of Information Resources Management, and that the security officer position will have authority "extending beyond headquarters operations." The Bureau also identified the additional duties of the security officer.

Regarding software development and change control, the Bureau said that it was "expanding and documenting improved procedures" for controlling software development and changes to existing software.

Based on the Bureau's response, we consider Recommendations A. 1, A.2, A.3, B. 1, C. 1, D. 1, D.2, E. 1, F. 1, G. 1, H. 1, and I. 1 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, we request that the Bureau respond to Recommendation J.l, which the Bureau did not specifically address. (See Appendix 3 .)

Additional Comments on Audit Report

In the response, the Bureau stated that Audit Report 97-I-90, which we identified in the Prior Audit Coverage section of our report, had not been "formally transmitted" to the Bureau of Indian Affairs by the Office of Inspector General and that the Bureau was not provided an opportunity to respond to the report. The Bureau requested that this fact be noted, and we have revised our report accordingly. As previously stated, however, the Office of the Special Trustee for American Indians, to whom Audit Report 97-I-90 was issued, advised that it provided a copy of the report to the Deputy Commissioner of Indian Affairs for consideration. Neither this fact nor the fact that the audit report identified weaknesses in the Bureau's information systems was disputed in the Bureau's response to this report.

Also, the Bureau said that specific pages of our report "would lead the reader to assume that Bureau management was solely responsible for the funding and staffing deficiencies within

the Office of Information Resources Management which directly contributed to the control weaknesses identified in the report," even though the Congress "denied" requested fiscal year 1996 funding increases for the Bureau's Central Office and reduced the fiscal year 1996 funding level "by approximately 25 percent below" the fiscal year 1995 level. We agree that the Congress reduced the Bureau's funding level; however, it did not specifically identify the functions within the Central Office that Bureau management should reduce. Considering that the Bureau recognized that "previous Departmental reviews had determined that OIRM [Office of Information Resources Management] was significantly underfunded at the pre-1996 levels," we believe that the Bureau's decision not to reallocate funding to the Office of Information Resources Management contributed to the weaknesses identified in our report.

The Bureau also requested that, if the "multiple" recommendations in our report relating to physical controls, user access, access to the UNISYS computer, segregation of duties, and system software are referred for tracking of implementation, they should be consolidated into one recommendation: "migration of mainframe data processing to U.S.G.S. [U. S Geological Survey] " However, we cannot comply with this request. While we agree that implementation action of "conversion of the mainframe data processing to the U.S.G.S. host computer" would be the first step in correcting the problems identified, other corrective actions are needed to fully implement the multiple recommendations. We therefore will refer all of the recommendations separately for tracking of implementation.

In accordance with the Departmental Manual (360 DM 5.3), we are requesting a written response to this report by May 30, 1997. 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.

DETAILS OF WEAKNESSES AND RECOMMENDATIONS

SYSTEM SECURITY PROGRAM

A. System Security Program

Condition: During fiscal year 1996, the Center did not have a documented security implementation plan for the Bureau's automated information systems. Although the Center had developed a security implementation plan by November 1996, the plan did not meet the detailed requirements of Office of Management and Budget Circular A-130, Appendix III, "Security of Federal Automated Information Systems." For example:

- 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 in effect. Further, the security staff had not provided periodic computer security training to Bureau area and agency offices and other organizations, such as schools.

- Risk assessments had not been performed periodically or had not been performed when systems, facilities, or other conditions changed. Specifically, since 1990, only two risk assessments had been performed: a risk assessment of the Center's previous mainframe configuration was performed in 1990, and a risk assessment of the LANs of the Albuquerque Central Offices was performed in 1996.[1] While we determined that these assessments were adequate, we also determined that the Center had not implemented recommendations from the risk assessments,

- Assessments of the system security program's effectiveness were not performed periodically. Also, the system security program was not reviewed under the Federal Managers' Financial Integrity Act annual review process.

[1]The Central Offices are administrative offices such as the Operations Service Center and the Division of Accounting Management. The Bureau has Central Offices in Washington, D.C., and in Albuquerque, New Mexico.

SYSTEM SECURITY PROGRAM

- Major systems and applications were not always accredited by the managers whose missions they supported.

Criteria: The Computer Security Act requires Federal agencies to develop and implement plans to safeguard systems that maintain sensitive data. Also, Office of Management and Budget Circular A-l 30, Appendix III, details what should be safeguarded by a system security program and what should be included in the security implementation plan. Additionally, the National Institute of Standards and Technology's handbook, "An Introduction to Computer Security: The NIST Handbook," describes a system security program as a program that includes security policies and a related security implementation plan. According to the handbook, the system security program should establish a framework for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures.

Cause: Because the Bureau's automated information system security function was within the Center, the function did not have adequate independence and authority to implement and enforce a Bureauwide system security program. The security staff consisted only of the automated information security officer and another staff person. Most of their time was spent in administering security at the Center and administering user access to the computer systems. Additionally, the 1996 risk assessment recommended that the system security function be directly responsible to the Commissioner, Bureau of Indian Affairs, which had not been accomplished by the end of our review. However, we believe that, at a minimum, the position should be elevated to report directly to the Director, Office of Information Resources Management.

Effect: The lack of an effective system security program prevents assurance that established controls can be relied upon to protect mission-based, sensitive computer systems.

SYSTEM SECURITY PROGRAM

Recommendations:

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

1. The automated information system 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.

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.

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.

SYSTEM SECURITY PROGRAM

B. Personnel Security Policies and Procedures

Condition: Personnel security policies and procedures were not adequate. Specifically:

- Personnel in sensitive or critical ADP positions, such as system programmers 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.

- 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 an employee was transferred.

Criteria: Office of Management and Budget Circular A-130, Appendix III, requires agencies to establish and manage personnel security policies, standards, and procedures that include requirements for: (1) screening individuals who participate in the design, development, operation, or maintenance of sensitive applications or who have access to sensitive data and (2) ensuring that access to computer systems is removed when employees terminate their employment or when employees are no longer in positions requiring such access. Additionally, the Departmental Manual (DM 441, "Personnel Suitability and Security Requirements") requires that background investigations be performed for security clearances before employees are placed in sensitive or critical ADP positions and that subsequent investigations be performed based upon the sensitivity or the criticality of the position.

Cause: The Bureau had established procedures for requiring background investigations for ADP positions that were sensitive and critical. However, the procedures were not implemented or enforced. Further, we did not find formal policies or procedures, such as requiring the deletion of the user ID from the security database during the exit clearance process, that required supervisors to notify the application owner or manager or Center security staff

SYSTEM SECURITY PROGRAM

when employees' employment was terminated or an employee was transferred.

Effect: Without adequate security-related personnel policies, the Bureau increases the risk that system operations and data could be impaired or compromised by individuals or by employees whose employment has been terminated or who have been transferred.

Recommendation:

We recommend that the Assistant Secretary for Indian Affairs 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.

ACCESS CONTROLS

C. Resource Classification

Condition: The Bureau had not classified its computer resources to determine the level of security that should be provided by the Center.

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

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

Effect: If information resources are not classified according to their criticality and sensitivity, there is no assurance that the Center was providing the most cost-effective means to protect the computer resources.

Recommendation:

We recommend that the Assistant Secretary for Indian Affairs 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.

ACCESS CONTROLS

D. Physical Controls

Condition: Physical controls, such as monitoring physical access to the Center and performing housekeeping functions for the computer operations room that houses the mainframe computers, LAN equipment, and daily backup tape libraries, were not adequate. For example:

- The Center was located within a Federal building (which also houses U.S. Courts) that allows 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 keycards, and access into the Center was monitored by video cameras. However, visitors, such as custodial (contractor) personnel and building managers, had been provided the keycards and therefore had unmonitored access while in the Center.

- General housekeeping and maintenance of the computer operations room were performed only weekly. This weekly schedule was inadequate because of the failure to remove potential fire hazards caused by combustible supplies and by dust produced by paper used in the printer, which was also housed in the computer operations room.

Criteria: The Department of the Interior Automated Information Systems Security Handbook, when addressing control for personnel access to computer facilities, states:

> Access by visitors, equipment maintenance personnel, and other individuals not directly involved with managing or operating a sensitive AIS [automated information system] installation will be controlled by individual authorization. It is recognized that different procedures and restrictions will be required for various categories of visitors; however, all access by other than assigned personnel will be monitored.

Additionally, the Handbook states that "within the facility, good housekeeping and operating procedures are prerequisite to maintaining a noncombustible

ACCESS CONTROLS

environment" and that operations such as "bursting and collating," which increase the potential for tire, should be restricted.

Cause: The Center was understaffed; therefore, Center personnel were not able to adequately monitor the activities of visitors. Also, the Bureau had reduced funding available to the Center; therefore, more frequent housekeeping services could not be obtained.

Effect: The deficient physical controls increased the risk of unauthorized access and damage to and destruction of sensitive hardware, software, and data.

Recommendations:

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

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

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.

ACCESS CONTROLS

E. User Access

Condition: Security staff and application owners did not periodically review user access authorizations to ensure that users' levels of access to the mainframe computers were appropriate.

Criteria: The Center's policy requires security staff to obtain written documentation from supervisory personnel and approval from application owners or managers before allowing users access to the mainframe computers.

Cause: The Center's policy did not require periodic reviews of users' access authority. In addition, the security function was understaffed and would not have been able to adequately perform the periodic reviews. Further, although RACF had been set up to automatically revoke user IDs after 180 days of inactivity, the IDs were not deleted from RACF because the security staff did not receive written notifications when employees terminated their employment or were transferred.

Effect: The Center had no assurance that user access was assigned at the appropriate level. Additionally, the Center increased the risk of unauthorized access and damage to and destruction of computer hardware, software, and data because of the time period between when an employee leaves and when the employee's access is automatically deleted.

Recommendation:

We recommend that the Assistant Secretary for Indian Affairs 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.

ACCESS CONTROLS

F. Access to the UNISYS Computer

Condition: 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,

Criteria: The Department of the Interior's "Automated Information Systems Security Handbook" recommends that passwords be changed every 90 days. Also, generally accepted industry standards recognize that passwords should be changed every 60 to 90 days for users who do not have sensitive privileges and every 30 days for users who do have sensitive privileges.

Cause: The Center has not acquired a security access control software package that can automatically require password changes and automatically revoke user IDs because the applications running on the UNISYS computer are to be moved to the IBM computer.

Effect: The effectiveness of the password as a control has been diminished, which increases the risk of unauthorized access to sensitive production information that resides on the UNISYS computer through password disclosure.

Recommendation:

We recommend that the Assistant Secretary for Indian Affairs ensure that a higher priority is given to moving the applications that reside on the UNISYS computer to the IBM computer.

SOFTWARE DEVELOPMENT AND CHANGE CONTROL

G. Software Development and Change Control

Condition: The software development and change control was 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, which was managed by the Bureau's Irrigation and Power Liaison and Control Section, 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 made aware of software modifications. Further, one member of the Center's systems staff could also move application software changes from test or development into production without the lead programmer's approval.

Criteria: The Departmental Manual (DM 385) describes system development life cycle management processes and change management controls. The Manual requires that a procedure be in place for approval and acceptance of changes and that a group or an individual be "responsible for ensuring that all changes have been properly evaluated."

Cause: The Bureau had not identified who was responsible and accountable for controlling application software development and changes.

Effect: The Bureau increased the risk that security features could be inadvertently or intentionally omitted or turned off or that processing of irregularities or malicious codes could be introduced. For example, the incorrect version of a program could be implemented, which could perpetuate outdated or erroneous processing.

Recommendation:

We recommend that the Assistant Secretary for Indian Affairs ensure that policies and procedures are developed and implemented which clearly identify the individuals responsible and accountable for application development and changes.

SEGREGATION OF DUTIES

H. Segregation of Duties

Condition: The duties for the systems 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. Specifically, we found that:

- System design, systems programming, data security, and data administration were accomplished or could be accomplished by one system programmer.

- Quality assurance/testing, change management, data security, and data administration could be performed by one system programmer.

- Quality assurance/testing, change management, and data administration could be performed by the National Irrigation Information Management System application programmers.

- Library management and computer operations were performed by the computer operators.

Criteria: Effective segregation of duties requires that each systems support function be performed by a different individual, thus ensuring that no one individual controls all critical stages of a process.

Cause: Center staffing was not sufficient to the extent that the segregation of duties could be adequately distributed. Center officials stated that, because of the Bureau's reduced budgetary resources, they were not able to fully staff the Center. However, we observed that in some of the functions, such as in applications programming, the staff were underutilized and that in other functions, the staff, such as computer operators, were utilized to the extent that the personnel were required to work overtime to ensure that this function was carried out.

SEGREGATION OF DUTIES

Effect: The lack of segregation of duties increases the risk that improper program changes could be implemented and that computer resources could be damaged or destroyed.

Recommendation:

We recommend that the Assistant Secretary for Indian Affairs ensure that staffing at the Center is evaluated and adjusted so that duties for critical system support functions are adequately segregated and fully utilized.

SYSTEM SOFTWARE

I. System Software Controls

Condition: The 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. 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 in monitoring system activities,

- One system programmer had "alter" access to system software, the System Maintenance Facility logs, and RACF logs. With this access, the programmer could alter the logging of his activities, as well as any other user activities. Thus the audit trails of system activities could be impaired or destroyed.

- RACF can be used to establish controls and monitor access to the computer resources. However, RACF had not been set up to effectively control access to the system resources. We found that one of the "start procedures" had been assigned the PRIVILEGED attribute. With this attribute, the started task can bypass all verification processing, including the security classification checks, and therefore affect the overall security of the system. Additionally, with the PRIVILEGED attribute, no logging or audit trail of this task was available. Further, no datasets, including the system parameter library, linklist libraries, master catalog, and the primary and backup files, were protected by RACF.

Criteria: Office of Management and Budget Circular A-130, Appendix III, requires that adequate audit trails exist so that an adverse impact on general support systems can be prevented or detected. Also, Federal Information Processing Publication 41, "Computer Security Guidelines for Implementing the Privacy Act of 1974," provides guidelines for system security and addresses the importance of having audit trails of all system activity.

SYSTEM SOFTWARE

Cause: Because the system programmer was responsible for setting up the IBM computer, the Center continued to rely solely on the programmer's expertise to ensure that the system was operating. Additionally, the security staff did not fully utilize RACF capabilities to monitor system programmer and system access activities.

Effect: The Center increased the risk of having the computer operating system and other computer resources altered without authorization and of not detecting the alteration through normal operating controls.

Recommendation:

We recommend that the Assistant Secretary for Indian Affairs 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.

SERVICE CONTINUITY

J. Service Continuity

Condition: 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. Although the Center has begun developing a service continuity plan for fiscal year 1997, the Center did not have a service continuity plan in place. Additionally, 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 or humidity.

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

SERVICE CONTINUITY

Cause: The Bureau did not ensure that necessary funding was provided to the Center to develop a contingency plan and to acquire or contract for an adequate off-site storage facility. Before fiscal year 1996, the Center had a contractor-developed contingency plan, and the contractor was responsible for performing disaster recovery tests, However, in fiscal year 1996, the Bureau decreased Center funding, and the contract was not continued. At the time of our review, the Center was negotiating for the acquisition of a computer site from which to perform disaster recovery testing.

Effect: The Center increased the risk of being unable to recover and resume critical operations should the system fail or disasters occur.

Recommendation:

We recommend that the Assistant Secretary for Indian Affairs ensure that a contingency plan is developed and tested and that funding is provided for acquiring a secure off-site storage facility.

United States Department of the Interior

OFFICE OF THE SECRETARY
Washington, D.C. 20240

MAR 1 0

Memorandum

To: Assistant Inspector General for Audits

From: Acting Assistant Secretary - Indian Affairs

Subject: Draft Audit Report, "General Controls Over Automated Information Systems, Bureau of Indian Affairs," (Assignment No. C-IN-BIA-009-96A)

The subject audit reviewed the general controls for the automated information systems, specifically those in place at the Operations Service Center in Albuquerque, NM. We request that a section of the Draft Report on prior audit coverage be modified, as indicated below and that information be added to the final report regarding the Bureau's budget situation.

Prior Audit Coverage

The identification or prior audit coverage includes only, the "Statement of Assets and Trust Fund Balances at September 30, 1995, of the Trust Funds Managed by the Office of Trust Funds Management, Bureau of Indian Affairs," (No. 97-I-96). While we do not dispute the fact that this audit identified weaknesses in our information systems, we would note that the audit findings were never formally transmitted to Indian Affairs, as the Office of Trust Funds Management was no longer part of the Bureau of Indian Affairs when the report was issued; indeed, the Office of Inspector General issued the audit which contained recommendations for action by the Bureau of Indian Affairs without either notifying us or allowing us the opportunity to respond. In view of the fact that normal procedures were not followed by the Office of Inspector General with respect to this report, we suggest that, at a minimum, this report identify the fact that the BIA was not provided an opportunity to respond to the report.

Funding and Staffing for the Center

In a number of places, the report would lead the reader to assume that Bureau management was solely responsible for the funding and staffing deficiencies within the Office of Information Resources Management which directly contributed to the control weaknesses identified in the report. For example: ". . . adequate funding and personnel were not provided to fully support the Center's mission" (p. 6); the system security program be "provided staff to perform the required duties" (p. 13); "The Center was understaffed. . ." (p. 18); ". . . the Bureau had reduced funding available to the Center. . ." (p. 18); ". . . the security function was understaffed. . ." (p. 19); "Center staffing was not sufficient to the extent that the segregation of duties could be adequately distributed" (p. 22); and "The Bureau did not ensure that necessary funding was provided to the Center. . ." (p.26).

As part of its action on the FY 1996 budget request, Congress denied all funding increases for Central Office; required the full absorption of pay cost increases; and also reduced funding for all BIA Central Office operations by approximately 25 percent below the FY 1995 level. This impacted all Central Office operations. The Center was particularly hard hit, because as the second largest headquarters office, their pay absorption was over $800,000. Previous Departmental reviews had determined that OIRM was significantly underfunded at the pre- 1996 levels. In fact, the FY 1996 budget request had included a total increase over the FY 1995 level of $3.5 million. The net result of the Congressional actions was that the Office of Information Resources Management was left with less than 60 percent of the resources that had been identified in the FY 1996 budget request.

We request that the report be revised to reflect the fact that it was action taken by Congress in cutting the budget request, not management decisions of the Bureau, that resulted in the severe shortage of staffing and funding for the Office of Information Resources Management.

Current Bureau Plans for Automated Information Systems

In accordance with the Administration's goal to reduce the number of computer operations centers across the Federal Government (OMB Bulletin #96-02, Consolidation of Agency Data Centers), the Bureau has been directed by DO1 to enter into an agreement with the U.S. Geological Survey to migrate all of the mainframe data processing to their host computer in Reston. The target date for completion of the transfer is December 1, 1997. In our discussions with OIG staff during and subsequent to the exit conference, it was generally agreed that in the pending transfer would be responsive to all of the recommendations contained in the audit with the exception of system security, personnel security, resource classification, and software development and change control. These recommendations are separately addressed in our response.

The' Bureau agrees with the recommendations contained in the draft audit report on Physical Controls, User Access, Access to the UNISYS Computer, Segregation of Duties, and System Software. The action that will be taken to implement these recommendations is the conversion of the mainframe data processing to the U.S.G.S. host computer. The conversion tasks that have been identified and the schedule for completion of the tasks is attached. Mr. Ed Socks has been designated as the project leader for the Bureau. Should these recommendations be referred to the Office of Financial Management for the tracking of implementation activities, we request that the multiple recommendations contained in the above-mentioned sections be consolidated into one recommendation: migration of mainframe data processing to U.S.G.S.

Our responses to the other recommendations contained in the report are provided below:

Svstem Security Program: We recommend that the Assistant Secretary - Indian Affairs ensure that:

1. The automated information system 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.

Bureau Resnonse: The Bureau concurs with the recommendation. 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. As part of this reorganization/redescription, the position of Security Officer will be elevated to report directly to the Director, OIRM. We will treat this position similar to that of the Bureau's Safety Officer who, while part of a headquarters organization, has authority extending beyond headquarters operations. The target date for completion of the reorganization plan is October 1, 1997, with an effective implementation date of December 1, 1997. Mr. Dale Bajema, Special Assistant to the Assistant Secretary and Mr. James Cain, Director, OIRM are the responsible officials.

** 2. A separate security function is established to administer the Center's security.

Bureau Resnonse: The Bureau does not concur. We believe that this recommendation would be appropriate if the Bureau were to continue to operate mainframe data processing. Since that function will be transferred to U.S.G.S., we believe that the Bureau Security Officer and his staffwill be able to manage the reduced security requirements of the Albuquerque OIRM site.

** 3. 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.

Bureau Resnonse: The Bureau concurs with respect to those functions which will remain the responsibility of the Bureau subsequent to the transfer of mainframe data processing to U.S.G.S. (e.g. telecommunications, local area networks and stand-alone microprocessors, and determinations as to sensitivity of data). The development of the policies and procedures will be the responsibility of the Bureau Security Officer, Mr. Jerry Belew. The policies and procedures will be completed by October 1, 1997.

** 4. 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.

Bureau Resnonse: The FY 1996 reduction-in-force eliminated OIRM staff capability to perform risk assessments. From the resources freed as a result of the transfer of data processing, and as part of the reorganization/redescription discussed above, positions will be established to perform the necessary risk assessments. Until such time as the reorganization/redescription is completed, we cannot identify a responsible official. The risk assessments will commence in July 1998 and the first assessment of all applications will be completed within 18 months of that date.

Personnel Security Policies and Procedures: We recommend that the Assistant Secretary - Indian Affairs 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.

** [OFFICE OF INSPECTOR GENERAL NOTE: As stated in our report, Recommendation A.2 has been deleted, and Recommendations A.3 and A.4 have been renumbered as Reconnendations A. 2 and A.3, respectively.]

Bureau Resnonse: The Bureau concurs. As a result of the audit, a review was conducted of the security clearances for those working at Operations Service Center; fully 2/3 did not have up-to-date clearances. 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; the responsible official is Mr. Jerry Belew.

To address the failure to delete user IDs when employees have transferred or have left the Bureau, two actions will be taken: (1) a report will be provided monthly to the Office of Information Resources Management of employees who have transferred within the Bureau so that system access can be reviewed and modified or revoked, if necessary; and (2) a report on employee terminations will be provided monthly so that system access can be revoked.

The responsibility for providing the reports to the Operations Service Center will be placed with the Personnel Office of the Office of Surface Mining as part of a reimbursable agreement that is in place to provide certain personnel support to the Bureau; the Acting Director, Office of Management and Administration, Mr. Jim McDivitt is responsible for providing this direction to OSM. The responsibility for revoking/modifying system access based upon the reports received rests with the Bureau Security Officer, Mr. Jerry Belew.

Resource Classification: We recommend that the Assistant Secretary - Indian Affairs 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.

Bureau Resnonse: This recommendation is essentially the same as the fourth recommendation which was made in the System Security section of the report. As indicated in our response to that recommendation, we will begin the risk assessments in July 1998.

Software Development and Change Control: We recommend that the Assistant Secretary for Indian Affairs ensure that policies andporcedures are developed and implemented w hich clearly identify the individuals responsible and accountable for application development and changes.

Bureau Response: The Bureau concurs. OIRM is in the process of expanding and documenting improved procedures in this area. This target date for completion is July 1, 1997; the responsible official is Mr. Dale Bajema, Special Assistant to the Assistant Secretary.

Any questions regarding the Bureau's response may be directed to Mr. James Cain, Director, Office of Information Resources Management.

Attachment

[NOTE: ATTACHMENT NOT INCLUDED BY OFFICE OF INSPECTOR GENERAL.]

STATUS OF AUDIT REPORT RECOMMENDATIONS

Finding/Recommendation Reference	Status	Action Required
A.l, A.2, A.3, B.l, C.l, D.l, D.2, E.l, F.l, G.l, H.l, and I.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.
J. 1	Unresolved	Provide a response to the recommendation. If concurrence is indicated, provide an action plan that includes target dates and titles of officials responsible for implementation. If nonconcurrence is indicated, provide reasons for the nonconcurrence.

ILLEGAL OR WASTEFUL ACTIVITIES 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-800-424-5081 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
1550 Wilson Boulevard
Suite 410
Arlington, Virginia 22209

(703) 235-9221

North Pacific Region

U.S. Department of the Interior
Office of Inspector General
North Pacific Region
238 Archbishop F.C. Flores Street
Suite 807, PDN Building
Agana, Guam 96910

(700) 550-7428 or
COMM 9-011-671-472-7279

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

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

HOTLINE

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