



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

AUDIT REPORT

**PERSONNEL AND PAYROLL PROCESSING
POLICIES AND PROCEDURES,
NATIONAL BUSINESS CENTER/
PRODUCTS AND SERVICES,
OFFICE OF THE SECRETARY,
DEPARTMENT OF THE INTERIOR**

**REPORT NO. 01-I-131
JANUARY 2001**

EXECUTIVE SUMMARY

**Personnel and Payroll Processing Policies and Procedures,
National Business Center/Products and Services,
Office of the Secretary, Department of the Interior
Report No. 01-I-131
January 2001**

The Department of the Interior's National Business Center/ Products and Services (NBC/PS), located in Lakewood, Colorado, implemented the Department's Federal Personnel Payroll System (FPPS) at the end of 1998. NBC/PS provides automated personnel and payroll services for its clients, the Department of the Interior and its bureaus and other Federal agencies, such as the Department of Education and the Social Security Administration. During 1999, NBC/PS processed payroll of approximately \$8 billion for approximately 175,000 Federal employees. NBC/PS receives funding through the Department of the Interior's working capital fund and through direct charges to client appropriations. During fiscal year 1999, NBC/PS charged its clients about \$29 million.

The objective of the audit was to determine whether NBC/PS's policies and procedures provided reasonable assurance that personnel and payroll transactions were processed and reported accurately and timely and were in compliance with applicable Federal laws and regulations.

We concluded that NBC/PS's policies and procedures generally provided for accurate and timely processing of personnel and payroll transactions in compliance with applicable personnel and payroll laws and regulations. In addition, we found that there may be opportunities to operate NBC/PS personnel and payroll processing and reporting functions more efficiently and to decrease the risk of unauthorized access to, modification of, and disclosure of personnel and payroll data and of critical systems not being recovered in the event of a disaster or a system failure. Based on our audit, NBC/PS began or completed developing a strategic plan for its operations, programing all required functions in FPPS, instituting all necessary security policies, and maintaining sufficient internal controls over software change management and separation of duties.

We made 12 recommendations for improving operations.

AUDITEE COMMENTS AND OFFICE OF INSPECTOR GENERAL EVALUATION

Based on NBC/PS's response to the recommendations, we considered seven recommendations resolved and implemented and five recommendations resolved but not implemented.



United States Department of the Interior

OFFICE OF INSPECTOR GENERAL
Washington, D.C. 20240

JAN 22 2001

AUDIT REPORT

Memorandum

To: Director, National Business Center, Office of the Secretary

From: Roger La Rouché *Roger LaRouche*
Acting Assistant Inspector General for Audits

Subject: Audit Report on Personnel and Payroll Processing Policies and Procedures,
National Business Center/Products and Services, Office of the Secretary,
Department of the Interior (No. 01-I-131)

INTRODUCTION

This report presents the results of our audit of personnel and payroll processing policies and procedures at the Department of the Interior's National Business Center/Products and Services (NBC/PS). The objective of this audit was to determine whether NBC/PS's policies and procedures provided reasonable assurance that personnel and payroll transactions were processed and reported accurately and timely, were in compliance with applicable Federal laws and regulations, and were processed efficiently. We performed this audit to support the Office of Inspector General's opinions on the annual financial statements of the Department of the Interior and its bureaus and offices.

BACKGROUND

During 1990, NBC/PS (formerly known as the Bureau of Reclamation's Denver Administrative Service Center), located in Lakewood, Colorado, began to develop the Federal Personnel Payroll System (FPPS) to replace the Department of the Interior's payroll and personnel system, PAY/PERS. By the end of 1998, NBC/PS had fully implemented FPPS.

FPPS, which resides on an IBM mainframe computer, was developed by the Bureau of Reclamation using Natural programming language with ADABAS¹ as the database

¹"ADABAS is a database management system from AG of North America that runs on IBM mainframes." (Alan Freedman, The Computer Glossary, fourth edition, AMACOM Division of the American Management Association, 1989, p. 9.)

management system. The enhanced features of FPPS include increased management information; paperless processing of personnel and payroll actions through on-line approvals; and immediate responses to on-line editing, updating, and query requests.

NBC/PS provides automated personnel and payroll services for its clients, the Department of the Interior and its bureaus, and other Federal agencies (see Appendix 1). Offices within NBC/PS that have responsibilities related to personnel and payroll processing are as follows:

- The ADP Services Division is responsible for managing the computer center where the IBM mainframe computer is located and for ensuring that telecommunications are operational and secure.
- The Payroll Operations Division (POD) is responsible for developing, implementing, operating, and maintaining the FPPS general support system,² known as the Automated Payroll System (APS), which resides on a Digital Alpha server. The APS includes the applications of Health Benefits Reporting, Thrift Lost Earnings, Debt Management, and Check Collection. POD is also responsible for reporting accurate payroll data to the clients and other Federal agencies, such as the Office of Personnel Management and the Department of the Treasury.
- The Applications Management Office's FPPS Program Management Division is responsible for developing, implementing, operating, and maintaining FPPS.
- The Management and Technical Service Division's Planning and Performance Support Branch is responsible for providing training for NBC/PS clients.

During 1999, NBC/PS processed payroll of approximately \$8 billion for approximately 175,000 Federal employees. NBC/PS receives funding through the Department of the Interior's working capital fund and through direct charges to client appropriations. During fiscal year 1999, NBC/PS charged its clients about \$29 million (about \$160 per account³).

SCOPE OF AUDIT

To accomplish our objective, we reviewed and tested policies and procedures that were in place during fiscal year 1999 for personnel and payroll processing at NBC/PS. We also interviewed NBC/PS personnel and NBC/PS contractor personnel, reviewed application and system documentation, analyzed network security, and evaluated service continuity

²Appendix III, "Security of Federal Automated Information Resources," of Office of Management and Budget Circular A-130, "Management of Federal Information Resources," defines a general support system as "an interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people."

³An account is equal to one employee's data maintained in FPPS.

procedures and testing. We did not review the internal controls over input that updates FPPS personnel data or the internal controls over data entry functions for time and attendance.

We also used Internet Scanner software developed by Internet Security Systems to identify vulnerabilities in NBC/PS's network. A list of the vulnerabilities identified by the Internet Scanner software was provided to NBC/PS management. For the vulnerabilities identified, NBC/PS management made appropriate changes to improve the security of its network.

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

PRIOR AUDIT COVERAGE

During the past 5 years, neither the Office of Inspector General nor the General Accounting Office has not issued any audit reports related to FPPS.

RESULTS OF AUDIT

We concluded that NBC/PS's policies and procedures generally provided for the accurate and timely processing of personnel and payroll transactions in compliance with applicable personnel and payroll laws and regulations. However, we identified areas needing improvement. Specifically, NBC/PS did not develop a strategic plan for NBC/PS operations, program all required functions in FPPS, institute all necessary security policies, and maintain sufficient internal controls over software change management and separation of duties. As a result, there may be opportunities to operate NBC/PS personnel and payroll processing and reporting functions more efficiently and to decrease the risk of unauthorized access to, modification of, and disclosure of personnel and payroll data and of critical systems not being recovered in the event of a disaster or a system failure.

Strategic Plan

NBC/PS management had not developed a strategic plan for NBC/PS operations. A strategic plan is needed to establish an agency's goals and match activities to mission and objectives, and it should include information on how to set priorities and allocate resources. Office of Management and Budget Circular A-123, "Management Accountability and Control," states, "Developing a written strategy for internal agency use may help ensure that appropriate action is taken throughout the year to meet the objectives of the Integrity Act."⁴

NBC/PS management said that they did not believe a strategic plan was necessary at the NBC/PS organizational level because it would be more appropriate to develop an NBC strategic plan that would include all services that NBC provides. We believe that without a strategic plan, NBC/PS is at risk of developing and implementing system enhancements

⁴The Federal Managers' Financial Integrity Act is codified in 31 U.S.C. § 3512.

using information technology that may not improve business processes and meet user requirements. Information technology that could be developed and implemented in system enhancements which would improve personnel and payroll processing includes distributed processing, use of electronic commerce applications, and a personnel and payroll system that integrates seamlessly with financial and management information systems.

Workarounds

To ensure that employees who were paid by FPPS were paid correctly and payroll information was reported accurately, NBC/PS personnel developed "workarounds."⁵ The purpose of the workarounds was to perform payroll functions that were required but were not part of FPPS. Additionally, applications such as Health Benefits Reporting and Thrift Lost Earnings were developed to operate on APS rather than FPPS, and these systems were not integrated.⁶ Further, spreadsheets were developed and used to correct payroll errors and to perform reconciliations. Examples of workarounds are as follows:

- A workaround was developed to ensure that variances were reconciled between the POD 200 report (a report of personnel costs created from four FPPS interface files) and the FPPS Labor Cost File (a file of personnel costs by program or activity as defined by each client that is interfaced with the clients' financial systems). Because the information for the POD 200 report and the FPPS Labor Cost File are generated from the same system, FPPS, the variances generated and the need for reconciling the variances may indicate that there are potential problems with data integrity or with programming.

- A workaround was developed to ensure that income taxes were consolidated and paid to appropriate state and local governments. NBC/PS staff who performed this consolidation effort said that the workaround takes approximately 40 hours of personnel time per biweekly pay period to complete. In comparison, this same function took about 1 hour of personnel time to complete as part of PAY/PERS, the replaced system.

- A workaround was developed to ensure that the Supplemental Semiannual Headcount Report submitted to the Office of Personnel Management was accurate. One field in this report is a count of all employees in an agency. FPPS was not programmed to calculate this field correctly; therefore, NBC/PS personnel had to manually determine the number of employees and correct a paper copy of the report. We found, however, that the headcount information for the Department of the Interior reported to the Office of Personnel Management for August 1999 was incorrect.

⁵ A workaround is a "tactic for accomplishing a task, despite a bug or other inadequacy in software or hardware, without actually fixing the underlying problem." (Microsoft Press, Computer Dictionary, third edition, Microsoft Press, Redmond, Washington, 1997, p. 511.)

⁶ Integrated refers to "a collection of distinct elements or components that have been built into one unit." (Alan Freedman, The Computer Glossary, fourth edition, AMACOM Division of the American Management Association, 1989, p. 366.)

Office of Management and Budget Circular A-127, "Financial Management Systems," describes a "mixed system" (such as FPPS) as an "information system that supports both financial and non-financial functions of the Federal government or components thereof." The Circular further states that "financial management systems must be in place to process and record financial events effectively and efficiently, and to provide complete, timely, reliable and consistent information." NBC/PS management said, however, that there were no plans for the immediate future to program functions in FPPS that are performed through workarounds because this may not be cost effective. We were not provided documentation to support that it was not cost effective to implement these FPPS changes. As a result, there was an increased risk that NBC/PS was not processing payroll transactions efficiently and effectively and may therefore not have been in compliance with Office of Management and Budget Circular A-127. There was also an increased risk that NBC/PS was not reporting accurate data.

Security Policies

NBC/PS management had not developed all the security policies necessary for FPPS and APS. Specifically, security policies had not been developed to adequately protect the NBC/PS telecommunications networks, sensitive data sent through electronic mail, and spreadsheets that support adjustments to FPPS data. In addition, security policies did not include an incident response plan and team, adequate preparation to recover critical functions and processes in the event of a disaster or a system failure, and assurance that risks were adequately assessed and managed. Further, system certifications, which certify that adequate security safeguards have been installed and imply the acceptance of risk, were not adequate, and system security plans had not been developed. Areas needing improvement in NBC/PS's security policies, plans, and practices are described as follows:

- Although NBC/PS had an informal firewall⁷ policy, which helped to ensure that its telecommunications networks were secure from probes and attacks from unauthorized users, NBC/PS did not have an overall site security policy. National Institute of Standards and Technology Special Publication 800-10, "Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls," states that a stand-alone policy "concerning only the firewall is not effective" because what is needed is a "strong site security policy."

NBC/PS management did not ensure that a site security policy was developed and implemented. Without a site security policy, there was an increased risk that NBC/PS telecommunications networks would not be adequately protected from unapproved access, misuse, or denial of service.

- NBC/PS did not have an adequate electronic mail usage policy for its employees and contractors to ensure that proprietary data, such as bank account and social security numbers, were sent to and accessed only by authorized individuals. Request for Comments

⁷A firewall is "a security system intended to protect an organization's network against external threats, such as hackers, coming from another network, such as the Internet." (Microsoft Press, Computer Dictionary, third edition, Microsoft Press, Redmond, Washington, 1997, p. 197.)

1244, "Site Security Handbook," referred to in National Institute of Standards and Technology Publication 800-10, states:

There may be levels of responsibility associated with a policy on computer security. At one level, each user of a computing resource may have a responsibility to protect his account. A user who allows his account to be compromised increases the chances of compromising other accounts or resources. . . . If the people you grant privileges to are not accountable, you run the risk of losing control of your system and will have difficulty managing a compromise in security.

Additionally, Office of Management and Budget Circular A-130, "Management of Federal Information Resources," states that agencies will "consider the effects of their actions on the privacy rights of individuals, and ensure that appropriate legal and technical safeguards are implemented." Although an electronic mail usage policy had not been developed, NBC/PS management said that a policy would be developed. By not having an adequate electronic mail usage policy, there was an increased risk that in the event of a security violation, NBC/PS management would not be able to show that their policy had been violated and therefore would have no recourse against the employees commensurate with the violation.

- NBC/PS had no security policies to adequately protect the data in spreadsheets used to support adjustments to FPPS data. Spreadsheets were developed to ensure that, on a case-by-case basis, Federal employees were paid correctly. We found that spreadsheet formulas, which were complex, were not protected from unauthorized changes; a management official was not held responsible for maintaining and updating the spreadsheets; spreadsheet formulas were not certified by managers responsible for ensuring data accuracy; and resultant payroll corrections were not approved prior to updating FPPS. National Institute of Standards and Technology Special Publication 500-171, "Computer User's Guide to the Protection of Information Resources," states, "In some cases, data is far more sensitive to accidental errors or omissions that compromise accuracy, integrity, or availability." Because formulas could become obsolete and data entry errors could be made and not be detected timely, there was an increased risk that employees could be paid incorrectly. During our review, NBC/PS management implemented policies and procedures that protected spreadsheet formulas from unauthorized changes, that established a process for revising and developing spreadsheets, and that provided for a third-party review of data being entered into FFS.

- NBC/PS did not have an incident response plan and a team to respond timely and efficiently to information system security incidents if an incident was caused by a computer virus, other malicious code, or a system intruder (either an authorized user performing an unauthorized act or an unauthorized user). Appendix III, "Security of Federal Automated Information Resources," of Office of Management and Budget Circular A-130 states:

When faced with a security incident, an agency should be able to respond in a manner that both protects its own information and helps to protect the

information of others who might be affected by the incident. To address this concern, agencies should establish formal incident response mechanisms.

NBC/PS management did not ensure that an incident response plan and a team were in place. Without an incident response plan and a team, there was an increased risk that security incidents would not be identified and, if identified, would not be addressed quickly and efficiently.

- NBC/PS management did not have an adequate disaster recovery plan for APS processing in the event of a disaster or a system failure. Appendix III of Office of Management and Budget Circular A-130 requires agencies to establish a comprehensive contingency plan and periodically test the capability to continue providing services and perform an agency function. Also, 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 mission." We found that a disaster recovery plan was developed for APS; however, the plan did not reflect the APS current environment, identify a specific location for APS to operate and connect to FPPS, and include an off-site location that is at least 1 mile from NBC/PS. As a result, there was an increased risk that all NBC/PS critical personnel and payroll processes supported by APS would not continue in the event of a disaster or a system failure.

- NBC/PS had performed its most recent risk assessments for FPPS and APS during fiscal year 1997. These risk assessments were not updated to reflect the current operational environments. During fiscal years 1997 to 1999 (through July 1999), FPPS software had been changed 13 times. The 1997 risk assessment for APS identified the system as a front-end processor⁸ for PAY/PERS rather than as the current general support system of POD. The risk assessments also did not address (1) all risks associated with FPPS and APS, (2) the selection of safeguards to mitigate risks, and (3) the acceptance of residual risk. Appendix III of Office of Management and Budget Circular A-130 states, "While formal risk analyses need not be performed, the need to determine adequate security will require that a risk-based approach be used." Appendix III further states, "The scope and frequency of the review should be commensurate with the acceptable level of risk for the system." Also, National Institute of Standards and Technology Special Publication 800-12, "An Introduction to Computer Security: the NIST Handbook," addresses the selection of safeguards to mitigate risk and the acceptance of residual risk. Risk assessments had not been performed since fiscal year 1997 because NBC/PS management stated that risk assessments are required only every 3 years by Appendix III of Office of Management and Budget Circular A-130. Without considering current operational environments and identifying all significant threats and vulnerabilities, the risk was increased that the most appropriate and cost-effective security measures needed to adequately protect the sensitive data maintained in FPPS and APS would not be implemented.

⁸A front-end processor is "a communications computer. It connects to the communications channels on one end and the main computer on the other." (Alan Freedman, The Computer Glossary, fourth edition, AMACOM Division of the American Management Association, 1989, p. 300.)

- NBC/PS had system certifications for FPPS and APS; however, the certifications were not signed by the appropriate responsible management official. NBC/PS had a "Sensitive Computer System Security Certification," which was signed by the manager responsible for development and maintenance of FPPS, and a "Sensitive AIS Security Certification Statement" on file for APS, which was signed by the manager responsible for APS daily operations. The Departmental Manual (375 DM 19) states that the management official responsible for application and system certification has the authority to accept the security safeguards and must possess authority to allocate the resources necessary to achieve acceptable security and to remedy security deficiencies. NBC/PS management stated that they believed the certifications were appropriate. However, we believe that the responsible management official should be at a level that is not directly involved with system development and maintenance or daily operations.

- NBC/PS did not have a system security plan for APS that was applicable to its current operating environment as a stand-alone system residing on a server rather than a front-end processor for PAY/PERS. A security plan is required by 5 U.S.C. § 552a to be developed for each Federal computer system that contains sensitive information. Also, National Institute of Standards and Technology Special Publication 800-18, "Guide for Developing Security Plans for Information Technology Systems," states that a computer security plan "is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements" and is to be designed to assist agencies in addressing the protection of systems to help ensure the systems' integrity, availability, and confidentiality. NBC/PS management said that the current version of the security plan was adequate. Without a security plan that is applicable to the APS operating environment, NBC/PS had little assurance that the current plan would address all of the management, operational, and technical controls necessary to protect the sensitive APS data.

- During our review, we used Internet Scanner software to determine whether NBC/PS's network had security vulnerabilities. Using the software, significant security vulnerabilities within NBC/PS's network were identified. We provided NBC/PS management with a list of the vulnerabilities, and NBC/PS management said that they would correct the deficiencies. At the same time, NBC/PS was also reconfiguring its network to improve security. Subsequent to NBC/PS's correcting its network deficiencies and reconfiguring its network, NBC/PS requested that we reuse Internet Scanner software to determine whether NBC/PS's network security had been improved. In reusing the software, we found that NBC/PS's network vulnerabilities had been significantly reduced.

Internal Controls

NBC/PS did not ensure that controls over changes to FPPS and APS application software were adequate and that duties were adequately separated for APS application programmers. These internal control issues are discussed as follows:

- Change management controls over FPPS and APS application software were not adequate. Specifically, NBC/PS management had not ensured that (1) controls were in place

over the FPPS emergency library,⁹ (2) controls were in place over FPPS and APS to ensure that all changes were authorized and appropriate, (3) all users who requested changes to FPPS were involved with testing to ensure that their requirements were met, and (4) adequate testing was performed prior to implementing each FPPS change release. Although FPPS personnel performed testing for each release of FPPS and had performed mini-regression testing¹⁰ for the latest release, system testing¹¹ had not been performed for FPPS releases. Federal Information Processing Standards Publication 106 states:

Testing standards and procedures should define the degree and depth of testing to be performed and the disposition of test materials upon successful completion of the testing. Whenever possible, the test procedures and test data should be developed by someone other than the person who performed the actual maintenance of the system. Testing is a critical component of software maintenance. As such the test procedures must be consistent and based on sound principles. The test plan should define the expected output and test for valid, invalid, expected, and unexpected cases. The test should examine whether or not the program is doing what it is supposed to do.

Also, prudent business practices require that custom-developed software be coded, tested, and accepted by users and management prior to moving the software into production. These practices should include unit testing to ensure that the changed software works properly when tested in isolation, systems testing to ensure that the changed software works when it is integrated with the total system, and integration testing to ensure that the total system works in the desired operating environment.

Without adequate controls over change management, there was an increased risk that critical software changes would not be made and that the applications would not perform as required by the users.

- NBC/PS management did not ensure that separation of duties was adequate for APS. Specifically, application programmers responsible for developing and making code changes to APS software were also responsible for moving these changes into production. Appendix III of Office of Management and Budget Circular A-130 requires that security

⁹Programs or data files are stored in an emergency library and used for processing following an emergency software change. (The Computer Language Company, Inc., Computer Desktop Encyclopedia, Version 9.4, 4th quarter, 1996.)

¹⁰Regression testing is "recommended," and it "extrapolates the impact of the changes on program and application throughput and response times from the before-and-after results using the test data and current performance." (Jeffrey L. Whitten, MS, CDP, Lonnie D. Bentley, MS, CD, and Victor M Barlow, MBA, CDP, Systems Analysis & Design Methods, third edition, Irwin, Burr Ridge, Illinois, 1994, p. 753.)

¹¹System tests, which are "essential," ensure that "application programs written in isolation work properly when they are integrated into the total system. It is not at all uncommon for programs that work perfectly by themselves to fail to work when combined with other, related programs." (Jeffrey L. Whitten, MS, CDP, Lonnie D. Bentley, MS, CD, and Victor M Barlow, MBA, CDP, Systems Analysis & Design Methods, third edition, Irwin, Burr Ridge, Illinois, 1994, p. 120.)

controls of personnel include separation of duties. Appendix III and National Institute of Standards and Technology Special Publication 800-12 define separation of duties as the division of roles and responsibilities and of steps in a critical function so that no one individual can undermine a critical process. Duties were not adequately separated because NBC/PS management did not have policies and procedures to ensure that APS application programmers' duties were adequately separated. As a result, there was an increased risk that inappropriate actions by application programmers would not be detected timely and that accidental or intentional actions by programmers could threaten the integrity of APS data and could interrupt processing.

Recommendations

We recommend that the Director, NBC:

1. Develop, implement, and maintain a strategic plan for NBC that includes personnel and payroll processing and operations.
2. Evaluate the necessity for workarounds that are used to supplement FPPS functions and determine whether these workarounds are more cost effective than adding these required functions to FPPS.
3. Develop, implement, and maintain a site security policy for NBC/PS.
4. Develop, implement, and maintain an electronic mail usage policy.
5. Document and maintain procedures to protect the data in spreadsheets and to review results from the spreadsheets that are used to update FPPS data.
6. Develop, implement, and maintain a formal incident response plan and team.
7. Ensure that NBC/PS contingency planning addresses APS processing in the event of a disaster or a system failure.
8. Perform risk assessments of FPPS and APS that represent the current operating environments and ensure that all risks and vulnerabilities are identified, the risks are reduced to an acceptable level, and any residual risks are accepted by senior-level management officials.
9. Ensure that system certifications for FPPS and APS are signed by senior-level management officials.
10. Develop an APS system security plan that reflects the current operating environment.

11. Document and implement policies and procedures to ensure that changes to FPPS and APS are authorized and appropriate and are adequately tested and that users are involved in testing.

12. Develop and implement policies and procedures to ensure that duties are adequately separated for APS application programmers.

NBC Response and Office of Inspector General Reply

In the September 1, 2000 response (Appendix 2) to the draft report from the Director of NBC, NBC concurred with the 12 recommendations. Based on the response, we consider Recommendations 5, 6, 8, 9, 10, 11, and 12 resolved and implemented and Recommendations 1, 2, 3, 4, and 7 resolved but not implemented. Accordingly, the unimplemented recommendations will be forwarded to the Assistant Secretary for Policy, Management and Budget for tracking of implementation (see Appendix 3).

Additional Comments on Report

In its response, NBC also provided additional comments on the report. We incorporated most of the changes as appropriate. However, our replies to NBC's specific comments on workarounds and internal controls are discussed in the paragraphs that follow.

Workarounds. NBC stated that it did "not perceive the POD200 report to be a 'workaround' . . . but as a system assurance report to check data variances."

The draft report did not state that the POD 200 report was the workaround. The workaround we discussed is the manual process to reconcile the POD 200 report to the Labor Cost File. The manual reconciliation has to be performed following each pay period and involves not only NBC/PS personnel but also NBC/PS's clients.

NBC also stated that it did not believe the facts in the draft audit report supported our conclusion that because NBC/PS uses workarounds, it may not be processing payroll transactions efficiently and effectively in accordance with Office of Management and Budget Circular A-127 and it may not be reporting accurate data.

In our opinion, NBC/PS's using workarounds does not ensure that FPPS is working efficiently and effectively to record financial events as required by Office of Management and Budget Circular A-127 and does not ensure data accuracy. For example, we found that for fiscal years 1998 and 1999, the Supplemental Semiannual Headcount Report submitted to the Office of Personnel Management contained inaccurate data in spite of the manual efforts to correct the Headcount Report.

Internal Controls. NBC said that we were "not accurate" in stating that system testing for FPPS releases (changes to FPPS) had not been performed. NBC further said that it believed the automated compares that were transferred to FPPS in 1999 when the conversions of clients' data to FPPS were completed satisfied the need for system testing.

Although the automated compares were transferred to FPPS after being tested, we do not believe that this process ensures that all FPPS releases have undergone system testing.

Since the report's recommendations are considered resolved, no further response to the Office of Inspector General is required (see Appendix 3).

Section 5(a) of the Inspector General Act (5 U.S.C. app. 3) requires the Office of Inspector General to list this report in its semiannual report to the Congress. In addition, the Office of Inspector General provides audit reports to the Congress.

**CLIENTS OF THE
NATIONAL BUSINESS CENTER/PRODUCTS AND SERVICES
FOR PERSONNEL AND PAYROLL SERVICES**

Department of the Interior:

Bureau of Indian Affairs
Bureau of Land Management
Bureau of Reclamation
U.S. Geological Survey
Minerals Management Service
National Park Service
Office of Aircraft Services
Office of Inspector General
Office of Surface Mining Reclamation and Enforcement
Office of the Secretary
U.S. Fish and Wildlife Service

Advisory Council on Historic Preservation
African Development Foundation
Commission of Fine Arts
Department of Education
Executive Residence/White House
Federal Labor Relations Authority
Federal Trade Commission
Harry S. Truman Scholarship Foundation
Inter-American Foundation
International Trade Commission
James Madison Memorial Fellowship Foundation
National Commission of Libraries & Information Science
National Education Goals Panel
Overseas Private Investment Corporation
Pension Benefit Guaranty Corporation
Presidio Trust
Securities and Exchange Commission
Selective Service System
Social Security Administration
Trade and Development Agency
U.S. Holocaust Memorial Council
Utah Reclamation Mitigation Conservation Commission



United States Department of the Interior

OFFICE OF THE SECRETARY
National Business Center
Washington, D.C. 20240-



Memorandum

SEP 1 2000

To: Robert J. Williams
Assistant Inspector General for Audits

From: Timothy G. Vigotsky *Tim Vigotsky*
Director, National Business Center

Subject: Draft Audit Report on Personnel and Payroll Processing, Policies, and Procedures, National Business Center/Products and Services, Office of the Secretary, Department of Interior (Assignment No. A-IN-OSS-001-99-M)

As required by Departmental Manual 360 DM 5.3, attached is the National Business Center's (NBC) written response to the subject audit report on Personnel and Payroll Processing, Policies and Procedures.

We concur with all of the recommendations in the audit report. Of the twelve recommendations seven have already been implemented. The schedule proposed for implementing the remaining recommendations is contained as Attachment 1. This schedule recognizes some of NBC's existing commitments; primarily the consolidation of all mainframe activities to one ADP center during fiscal year 2001. In addition, with respect to recommendations requiring outside coordination and concurrence (as with an employee union or backup hotsite), we have identified target implementation dates which are contingent in part upon actions by external organizations.

While the auditors did a thorough and professional job, we believe there are some misunderstandings relating to some of the descriptions of conditions or NBC management positions in the body of the audit report, as some of our comments to the preliminary draft audit report were not incorporated. We have responded to these issues in Attachment 2.

The auditors made several helpful recommendations and alerted us to some potential problem areas that needed our attention. We appreciate the constructive input of your staff and the opportunity to provide comments on the audit recommendations.

If there are any questions or concerns, please contact Rick Koeber, Acting Director, NBC Products and Services at (303)-969-7210.

Attachments (2)

cc. D-2980 G. Dragseth

Attachment 1
Page 1 of 4
August 30, 2000

RECOMMENDATIONS AND RESPONSES

Recom. #1 "Develop, implement, and maintain a strategic plan for the NBC that includes personnel and payroll processing operations."

Response: Concur. NBC is currently developing a strategic plan. It is expected to be published by October 31, 2000.

Recom. #2 "Evaluate the necessity for workarounds that are used to supplement FPPS functions and determine whether these workarounds are more cost effective than adding these required functions to FPPS."

Response: Concur with intent. The server based applications which we use to supplement FPPS will be evaluated by January 1, 2001.

Comment: Evaluating the cost effectiveness of system changes is already part of the prioritization process to determine what changes will be made to FPPS. However, while a major criteria, cost effectiveness is not the sole criteria by which decisions about FPPS changes are made. Client change requests, legislative changes, and the availability of limited resources must also be considered.

Recom. #3 "Develop, implement, and maintain a site security policy for NBC/PS."

Response: Concur. The target date for development and implementation of the policy is October 1, 2001. Maintenance of the plan will be ongoing indefinitely and will be accomplished through periodic reviews.

Comment: The NBC P/S organization presently has numerous security policies and procedures in place. These policies cover physical access controls, (IT-SEC-POL-00A), DSAF Security Requirements, (IT-SEC-POL-00B), System Access Controls (IT-SEC-POL-00C & 002), Access to Datasets, Resources, and Functions (IT-SEC-POL-001), Personnel Security and Suitability requirements (IT-SEC-POL-003), and Data Center Network Firewall Policy (IT-SEC-POL-004). We recognize that these plans address pieces of our site security policies and procedures and that there is a need for a comprehensive site security policy.

Recom. #4 "Develop, implement, and maintain an electronic mail usage policy."

Attachment 1
Page 2 of 4
August 30, 2000

Response: Concur. The target implementation date is January 1, 2001.

Comment: A draft Electronic Mail Usage Policy was completed in March 2000. The draft has been reviewed by NBC P/S Management. However, because such a policy could significantly impact work procedures or conditions, it has also been forwarded to the labor bargaining unit for input and comment. After review by the labor bargaining unit and further re-negotiations with management (if necessary), the policy will be issued and distributed to all NBC/PS employees.

Recom. #5 "Document and maintain procedures to protect the data in spreadsheets and to review results from the spreadsheets that are used to update FPPS data."

Response: Complied. The recommendation has been implemented.

Comment: Payroll Operations Division Internal Operating Procedures entitled "Utilizing Spreadsheets" have been revised to provide control and oversight of spreadsheet formulae and results. The procedures were approved by the Acting Director, National Business Center Products and Services and were forwarded to the Office of Inspector General on July 31, 2000.

Recom. #6 "Develop, implement, and maintain a formal incident response plan and team."

Response: Complied. The recommendation has been implemented.

Comment: The NBC has had the information sharing piece of an Incident Response Capability, as required by OMB A-130 in place for several years. The Security Manager is on e-mail distribution lists for Security Alerts and Bulletins distributed by various organizations such as FedCIRC, CERT, SANS, etc. Pertinent bulletins are distributed internally to NBC/PS technicians for review. In addition, DOI signed a formal Letter of Agreement with FedCIRC in December 1998 to establish a formal mechanism for incident coordination and information warehousing and dissemination. NBC P/S is covered under this formal DOI agreement. In March of 2000, NBC/PS issued a formal Computer Security Incident Response Capability Charter (IT-SEC-DIR-001) and formed a formal Incident Response Team comprised of members from each division. Maintenance of the overall incident response plan will consist of periodic team meetings and will include training of team members.

Attachment 1
Page 3 of 4
August 30, 2000

Recom. #7 "Ensure that NBC/PS contingency planning addresses APS processing in the event of a disaster or system failure."

Response: Concur. The target date for completing the logistical arrangements and revisions to contingency plans is January 1, 2001.

Comment: A contingency plan for the Payroll Operations Division (POD) Alpha Server (upon which APS processing occurs) was already in existence prior to the audit. However, this plan did not call for an emergency relocation site for the Alpha which is more than one mile from NBC. Internal plans are in process to identify a specific site for emergency relocation of the Alpha server. In the event of disaster, the Alpha hardware would be shipped directly to the emergency site by Compaq Computer Corporation. This is covered under a "recover-all" contract with Compaq which requires replacement of the Alpha system within 24 hours of a disaster situation. The contingency plans for the Alpha server and any other affected contingency plans will be revised once specific site arrangements have been finalized.

Recom. #8 "Perform risk assessments of FPPS and APS that represent the current operating environments and ensure that all risks and vulnerabilities are identified, the risks reduced to an acceptable level, and that any residual risks are accepted by senior-level management officials."

Response: Complied. The recommendation has been implemented.

Comment: Risk assessments have been completed for FPPS and APS which address current operating environments. These assessments were performed during FY 2000 and were reviewed and approved by the Acting Director, National Business Center Products and Services on July 5 and 6, 2000.

Recom. #9 "Ensure that system certifications for FPPS and APS are signed by senior-level management officials."

Response: Complied. The recommendation has been implemented.

Comment: An FPPS system certification was signed by the Acting Director of Personnel, Office of the Secretary on August 29, 1997. This certification also recommended that FPPS deployment should begin in the Department of the Interior. Also, Sensitive Security Certification Statements were completed, reviewed, and approved by the Acting Director, National Business Center Products and Services on July 6, 2000.

Attachment 1
Page 4 of 4
August 30, 2000

Recom. #10 "Develop an APS system security plan that reflects the current operating environment."

Response: Complied. The recommendation has been implemented.

Comment: The recently completed Sensitive System Security plan that was completed for the Payroll Operations Division (POD) Alpha Server (upon which APS processing occurs), was performed using the current APS operating environment. The plan was completed in June of 2000, was reviewed by the Chief, Payroll Operations Division, and was approved by the Acting Director, National Business Center Products and Services on July 6, 2000.

Recom. #11 "Document and implement policies and procedures to ensure that changes to FPPS and APS are authorized and appropriate and are adequately tested and that users are involved in the testing."

Response: Complied. The recommendation has been implemented.

Comment: FPPS has a formal change management process that documents the request and authorization process. Changes are reviewed for appropriateness by the FPPS staff and then submitted to the FPPS Users Group for approval and prioritization. In January of 2000, quality assurance testing procedures were expanded to include an entire test database where a "regression test" is now performed of a production pay period prior to a new release of FPPS software being implemented. In May of 2000, the testing was expanded to include two production pay periods in order to verify re-computation results. Emergency migration procedures were also revised in May 2000 to ensure that only authorized changes are moved into production databases. The Payroll Operations Division (a principal FPPS user) has tested all proposed FPPS changes that impact its operations and client interface files are available to clients for validation of the test results of new FPPS releases. A formal agreement with Social Security Administration has been recently negotiated which documents their involvement in the testing process.

Payroll Operations Division Operating Procedures have been revised to outline processes and responsibilities for change management and testing for any changes to the Payroll Operations Division's Alpha Server applications. All Alpha Server users are internal to the Payroll Operations Division and have been included in testing applicable Alpha software changes.

Recom. #12 "Develop and implement policies and procedures to ensure that duties are adequately separated for APS application programmers."

Response: Complied. The recommendation has been implemented.

Comment: Payroll Operations Division Internal Operating Procedures have been revised to provide for adequate separation of duties for application programmers on the POD Alpha Server. The procedures were approved by the Acting Director, National Business Center Products and Services, have been distributed internally, and were forwarded to the Office of Inspector General on July 31, 2000.

Attachment 2
Page 1 of 3
August 30, 2000

COMMENTS ON DESCRIPTION OF CONDITIONS

The following comments respond to specific paragraphs of the audit report which we feel could be misleading to reviewers. In some cases, the paragraphs in question reflect conclusions inaccurately drawn from processes or data as to management intent or omissions regarding specific actions. Other references respond to factual rather than perceptual inconsistencies which we feel should be corrected prior to issuance of the final audit report.

Because our earlier attempts to reconcile these issues were not reflected in the draft report, we feel it appropriate to highlight specifically the narrative descriptions which we consider potentially misleading and recommend that they be modified in the final audit report.

Page 2 Paragraph 1 For consistency, the report should state that NBC/PS developed FPPS rather than BOR. While we were part of BOR during FPPS development, the audit is directed to NBC/PS.

Page 4 Paragraph 3 We do not agree with the statement that NBC PS developed "workarounds" to perform reconciliation's on historical data. The term "workarounds" refers to shortcuts or other actions taken to accomplish a task in spite of rather than correcting an underlying bug or other inadequacy in software or hardware. As such, use of this term is misleading in several places in the draft report and tends to create a negative impression of actions or procedures we feel to be appropriate.

For example, in connection with conversion of data from PAYPERS to FPPS, the actions referred to as "workarounds" in some cases related to historical data not previously maintained by PAYPERS rather than a shortcut to avoid fixing a software problem. Management made conscious design decisions during the development of FPPS to not convert the historical data from PAY/PERS to FPPS. There was not and is not a one to one match with data elements maintained in each of the two systems. FPPS had automated more personnel/ payroll processes and had more security accesses requiring additional data fields beyond what PAY/PERS had on their data files. It was not feasible to attempt to reconstruct historical data for conversion purposes when that data had not been tracked or collected anywhere.

Page 4 Paragraph 4 We do not perceive the POD200 to be a "workaround". The POD200 report is actually a system assurance report to check data variances. We

consider this a normal part of the data reconciliation process and not a "workaround".

Page 5 General There are a number of functions which solely support Payroll operations users (such as Health Benefits Reporting and Thrift Lost Earnings). Our external FPPS clients would have no need for these POD specific functions. When these functions can be provided for POD through a relatively inexpensive Alpha database server, it is unlikely that converting all this data and incorporating all these functions into FPPS would be cost effective from the client's perspective. However, we are not opposed to preparing a formal cost-effectiveness study document that would address incorporating certain APS functions into FPPS.

Page 5 Paragraph 1 Information on consolidating and paying state and local income taxes was further reviewed for accuracy. This process now takes about 8 hours rather than 40 hours as stated in the audit report. That time frame is still considered unacceptable and a change request has been initiated to incorporate this function into FPPS. We appreciate the auditors bringing this matter to our attention.

Page 5 Paragraph 2 The Supplemental Semi-Annual Headcount Report did have a problem which was corrected in FPPS release 1.11.

Page 5 Paragraph 3 The statement attributed to NBC/PS Management is not accurate. NBC Management is continually evaluating FPPS programming changes which can result in better or more cost effective delivery of services, including those which would be necessary to replace the perceived "workarounds". FPPS programming change decisions are driven by a number of factors including client requirements, legislative changes, availability of resources, as well as cost effectiveness. Cost effectiveness of a change is only one priority among a number of competing ones. Additional management comments are noted under Audit Recommendation #2.

Page 5 Paragraph 3 The auditors raised some valid concerns about the Semi-Annual Headcount report and the time it takes to consolidate state and local income taxes. In both cases, we have taken action to correct the problems. We don't believe the facts support the negative conclusion that NBC/PS "may not be in compliance with OMB A-127", or is "not reporting accurate data". We feel that the tone of the concluding sentences in this paragraph is more negative than the facts in the finding warrant.

Page 5 Paragraph 4 We agree that some of our security policies could have been improved. However, we feel that this paragraph portrays an overly negative impression to readers unfamiliar with our policies and accomplishments in this area. For example, while Page 6 of the draft report addresses the inadequacy of

our existing email management policy, its wording could leave readers with the erroneous impression that we had no email management policies.

Another example which illustrates our concern involves the sentence in the draft report "NBC/PS management had not developed necessary security policies for FPPS and APS." System security plans had been in place prior to the audit for all our major systems. The audit recommendations speak to improvements that could be made in our existing security plans. Again, however, we feel that the tone of this paragraph could create a false impression about the level of security in place at the time of the audit.

Page 6 Paragraph 1 The statements attributed to NBC/PS Management are not accurate. We request that this sentence be deleted from the audit report.

Page 7 Paragraph 1 We have revised our procedures to track spreadsheet changes through a formally documented work request. We believe this will provide a tracking system to ensure accountability and data accuracy whenever changes to spreadsheet formulate are necessary.

Page 7 Paragraph 4 The statements attributed to NBC/PS Management are not accurate and should be deleted. Our belief at the time of the audit was that our incident response requirements were met through a 1998 agreement which the Department of the Interior had signed with FedCIRC as well as by information sharing among Security Officers in other bureaus, businesses and installations. We have, however, since established a formal incident response team internal to NBC/PS.

Page 8 Paragraph 2 The sentence quoting "Further, the manual states that the authorization of a major application and general support system will generally occur at a very high management level.... is not relevant to the topic of sensitive system certifications and should be deleted." This rest of the paragraph has to do with sensitive system certifications which is a separate process from authorizing an application for use. We provided documentation to the auditors showing that the Director of the Departmental Personnel office authorized the deployment of FPPS in August 1997. We do agree, however, that sensitive system certifications should be made at a high management level within the NBC, but feel that the Assistant Directorate level is appropriate.

Page 10 Top The statement that "....system testing had not been performed for FPPS releases....." is not accurate. The audit defines the term "system testing" as ensuring that application programs written in isolation work properly when integrated into a total system. Multiple parallel and automated quality assurance testing was performed throughout the conversion of all clients to FPPS. This testing included full pay period parallels and automated compares. There were defined expected results and unexpected results which were researched. Once

conversions were complete, these automated compares were transferred to FPPS in 1999. Our testing plans very much consider how FPPS releases would perform as part of a total system as well as in isolation. We are unclear on what additional testing would have been appropriate or expected.

STATUS OF AUDIT REPORT RECOMMENDATIONS

Finding/Recommendation Reference	Status	Action Required
5, 6, 8, 9, 10, 11, and 12	Implemented.	No further action is required.
1, 2, 3, 4, and 7	Resolved; not implemented.	No further response to the Office of Inspector General is required. The information regarding the status of these recommendations will be provided to the Assistant Secretary for Policy, Management and Budget for tracking of implementation.

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

Internet Complaint Form Address

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

Within the Continental United States

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

Our 24-hour
Telephone HOTLINE
1-800-424-5081 or
(202) 208-5300

TDD for hearing impaired
(202) 208-2420

Outside the Continental United States

Caribbean Region

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

(703) 235-9221

Pacific Region

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

(671) 647-6060

HOTLINE

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

Toll Free Number
1-800-424-5081

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

