3166l

UNITED STATES GENERAL ACCOUNTING OFFICE
WASHINGTON, D.C. 20548

ACCOUNTING AND FINANCIAL
MANAGEMENT DIVISION

JULY 12, 1985

B-218842

The Honorable John R. Block
The Secretary of Agriculture

Dear Mr. Secretary:

Subject: Improvements Needed in General Automated Data Processing Controls at the National Finance Center (GAO/AFMD-85-38)

As part of our present and on-going evaluations of the U.S. Department of Agriculture's (USDA's) central accounting system, we assessed the adequacy of selected general automated data processing (ADP) controls at the National Finance Center (NFC) in New Orleans, La., where this system is operated and maintained. The NFC performs all payment functions for the administrative expenses of Agriculture, and it provides accounting services for most USDA agencies. General controls apply to all processing carried out in a data processing facility and are independent of the computer applications.

USDA's central accounting system consists of over 20 payment, collection, and financial accounting and reporting systems. According to NFC statistics, over 13 million transactions involving over $4 billion in payments and $200 million in collections were processed by these component systems in calendar year 1983.

Adequate general ADP controls are essential for ensuring the reliability of and security over the data processed by these computer-based systems. This letter is to advise you of several areas in which we found general ADP controls to be weak or nonexistent. We did not attempt to determine the cause of the weaknesses, nor did we assess the total effect that could result from existing conditions. Specifically, we found that:

--NFC did not have a formal disaster recovery and backup processing plan to ensure continued operations of its financial and personnel systems.

--Computer program documentation for the payroll/personnel, billings and collections, and miscellaneous payments systems was not current or complete, which hindered system maintenance.

032533

--NFC programmers did most of the testing on their own program changes, with little or no supervisory review or independent certification. This provides opportunities for inaccurate program changes.

--Some NFC personnel had unrestricted access to both computer data files containing payroll, financial, personnel and other sensitive information and to computer programs which perform the necessary functions of paying employees and collecting for services. Because of this access, both data and programs could be fraudulently altered, and NFC's compliance with the confidentiality provisions of the Privacy Act of 1974 could be compromised.

On April 13, 1984, we initially discussed our findings with the NFC Director and his staff, who generally agreed that improved controls were needed. Since that meeting, NFC has developed corrective action plans, and was still working to resolve some of these weaknesses as of May 1985 (see enclosure).

Passage of the Federal Managers' Financial Integrity Act of 1982 reaffirmed the importance of effective internal controls. This act requires executive agency heads to evaluate agency internal control systems and report annually to the Congress on whether they adequately meet prescribed standards. As part of this process, NFC stated in a November 13, 1984, report to Agriculture's Office of Finance and Management (OFM) that it had begun tracking our findings, and formulating and reporting corrective actions.

In that report, the NFC informed OFM of our findings relative to programmer access, program documentation, program certification, and disaster procedures. NFC also provided information on its action plans to address the weaknesses as well as scheduled completion dates. However, our subsequent inquiries have indicated slippages in some of the scheduled completion dates. We believe top management emphasis is needed to ensure completion and implementation of all actions to resolve our concerns.

OBJECTIVE, SCOPE, AND METHODOLOGY

Our review's objective was to assess NFC's general controls over its data processing operations. Using control objectives we have developed, we evaluated the extent to which NFC had established adequate control techniques in the following general ADP control areas: (1) organizational controls, which include separation of duties and personnel policies; (2) application systems maintenance, which includes controls over documentation, changes, testing, and access to programs; (3) data center operations, supervision, and review; (4) system software, which entails controls over modifications, testing, and access of system programs; and (5) data center protection which includes physical access to the center, backup of data and programs, and disaster recovery.

Through discussions with NFC system and application programmers and ADP security and operations personnel, and review of NFC ADP system procedures and directives, we identified the extent of the internal control techniques that are in place for the five areas. Where appropriate, we tested compliance with stated control techniques by observation and by reviewing processing logs, forms, system outputs, and other documentation. We selected the payroll/personnel, miscellaneous payments, and program billings and collections systems to assess general controls over application systems maintenance (i.e., the changes that are periodically made to programs which process the data). These systems were selected because of the high number of transactions and the amount of money involved. For example, during 1982 the NFC reported the following:

System	Document count	Dollars processed
Program Billings & Collections	1.3 million	$ 5 billion
Payroll/Personnel	5 million	$ 2.5 billion
Miscellaneous Payments	183 thousand	$ 841 million

Our work was done during March through May 1984. In early November 1984, we conducted a brief follow-up review on the status of NFC corrective actions by interviewing NFC officials responsible for the actions. Our work was performed in accordance with generally accepted government auditing standards. The following sections discuss the improvements needed.

NEED FOR DISASTER RECOVERY AND BACKUP PROCESSING PLANS

NFC did not have a formal contingency plan for disaster recovery and backup processing required by both the Office of Management and Budget's (OMB's) Circular A-71 (Transmittal Memorandum No. 1, dated July 27, 1978) and Federal Property Management Regulation (FPMR) 101-35.3. Consequently, there is little assurance that NFC could provide continuity of essential data processing support for USDA's payroll/personnel and payment and collection activities should events occur which would prevent normal operations.

The guidelines for ADP contingency planning are in Federal Information Processing Standards Publication (FIPS PUB) 87. Consistent with FIPS PUB 87, FPMR 101-35.3, and A-71, NFC needs to develop contingency plans which include

--appropriate response procedures in the event of fire, flood, civil disorder, bomb threat, or natural disaster to protect lives, limit damage, and minimize the impact on ADP operations;

--recovery procedures permitting rapid restoration of the ADP facility following physical destruction, major damage, or loss of data;

--backup procedures (including formal arrangements with an alternate, compatible ADP facility) to ensure essential ADP operations can be conducted after disruption to the primary ADP facility; and

--periodic review and testing of contingency plans.

NFC has recognized the need for contingency planning. Its five-year Plan covering fiscal years 1984-88 provided for the development by September 1986 of a model plan on recovering from a disaster affecting ADP systems. In a status briefing on June 1, 1984, the NFC Director and his staff advised us that an ADP contractor was being hired to help NFC develop its contingency plans and that such plans should be completed by October 1984. Our early November 1984 follow-up disclosed that a consultant had been hired and NFC now estimates that development of its contingency plans, selection of an alternate ADP backup facility, and testing of contingency plans will be completed by the end of May 1986.

NEED TO IMPROVE PROGRAM DOCUMENTATION

Computer program documentation for the payroll/personnel, program billings and collections, and miscellaneous payments systems was not current or complete. The objective of good documentation is to provide a clear, understandable description of the system and each program in a system. Good documentation increases the ease and accuracy of computer program maintenance and provides the basis for evaluating a system's internal controls. Documentation facilitates communication and may act as a deterrent to fraudulent manipulation of systems, which is usually easier to perform when there is little or no documentation.

If documentation is not complete or current, erroneous program changes may occur, since confusion can exist as to what is to be changed. As a result, processing may be performed incorrectly or control techniques performed by computer programs may be altered, deleted, or otherwise rendered inoperable by persons making changes.

We found that program documentation for the payroll/personnel system did not include:

--current program compile listings (the program actually used by the computer), program job control listings (the specific instructions that identify computer hardware needed), test data for coding changes (the data used to test program changes), and a description of program output;

--descriptions in the detail necessary to explain program functions; and

--flow diagrams that reflected the flow of data as it is processed through the system.

In addition, we found one instance in which the program code had become obsolete and served no useful purpose. This code had not been deleted from some payroll programs, and when payroll is being processed the programs are put in the computer's memory. This could cause excess memory to be used to maintain the code, and increase the cost of processing.

Although we found that the documentation for the billings and collections system and the miscellaneous payments system was considerably more complete and current than the payroll/personnel system, we identified missing documentation relating to program modifications. For example, we found that program documentation did not contain test data for program coding changes or even all required forms used to record program changes.

According to the NFC Management Control Division chief, NFC's documentation standards are in accordance with Departmental Information Processing Standards (DIPS), which are guidelines adapted from FIPS. However, in reviewing NFC documentation standards, issued April 25, 1984, we found inconsistencies between NFC's standards for documenting software and the guidelines described in FIPS PUB 38. For example, the description of control totals accumulated during processing to ensure data is not lost and the inclusion of the job control instructions are optional rather than required in NFC's standards. Also, the NFC standards do not require descriptions of interfaces with other programs or modules as does FIPS. In addition, the NFC standards do not address documentation of sensitive data and Privacy Act requirements related to disclosure of this data. These requirements are imposed by law (5 U.S.C. 552a(b)).

On March 1, 1984, we discussed our concern about the payroll/personnel system documentation with the NFC Director and his staff. In response, they stated that a certification group has been established to begin reviewing each computer-based system, as required by OMB Circular A-71. As a part of this review, documentation on each system and on a sampling of computer programs will be checked to ensure that program documentation is current and complete.

Certifications of payroll/personnel subsystems were scheduled for completion by May 1985. Our November 1984 follow-up disclosed that the completion date had been extended to August 30, 1985. Certification of other NFC systems is to begin when the payroll/personnel system is complete.

NEED TO IMPROVE PROGRAM CHANGE CONTROLS

NFC application programmers modify computer programs and test modifications with little or no review by supervisors or certification by independent third parties that the changes are proper. Additionally, no formal procedures exist for testing computer program changes.

By allowing programmers to modify computer programs with little or no review and to do their own testing, management is relinquishing an important means of ensuring system integrity. As a consequence, there is the potential for unscrupulous persons to make unauthorized program changes and in the process perform and conceal fraud.

Program change controls assure management that computer programs are not modified, even unintentionally, without proper authorization. In this way, there is assurance that the integrity and reliability of computer systems are maintained. According to FIPS PUB 31, "every change, even those involving only one (program) statement, should be authorized, approved, and documented with no exceptions."

NFC procedures require that all change requests receive supervisory approval before a change is made, except for emergency changes which are approved after the change has been made. Under either procedure, we found no evidence that program changes, once approved, are independently reviewed and tested to ensure that only the authorized change was made. We found that no formal testing standards and procedures existed and no certification group was performing this function.

On March 1, 1984, NFC established a system certification group and in May 1984, this group started reviewing a limited number of program changes by comparing the old program code to the new program code. However, this review was limited to programs with a small number of coding changes. Our November 1984 follow-up found that NFC had hired one staff person and was in the process of hiring three additional staff members to enable its certification group to perform program testing. Also, NFC planned to complete formal testing standards and procedures by December 3, 1984. Implementation of the standards and procedures with respect to both program changes and new programs was scheduled to begin January 20, 1985. We checked with NFC in early February, 1985 and were told that a draft had been issued for comment. In commenting on a draft of our report, the Assistant Secretary for Administration stated that a final application testing procedure should be implemented by July 1985.

NEED TO RESTRICT ACCESS TO DATA AND PROGRAMS

NFC programmers have access to production data files and production programs. Production data files include payroll, personnel, financial, or collection information which is being processed into the system. Production programs include the instructions to the computer on how to process this information.

By having the capability to access production data files and programs, programmers can more easily obtain detailed knowledge of the overall system. Thereby, they would find it easier to change programs or data which might result in fraudulent transactions.

Access to program data files and production programs should be granted because of an individual's need for such access. This access should be reviewed periodically. At NFC, programmers were granted open-ended access to production data files and programs during implementation of a system. However, the access was never removed after implementation.

NFC currently has programs with controls that can restrict access to production data and programs. These controls can limit access to the data base by time of day, day of the week, programs, section of the data base, or data element. However, NFC had not used these programs to restrict the access of programmers.

The NFC Director and his staff advised us on June 1, 1984, that a methodology had been developed to use the security software to control programmer access to production data files. Our November 1984 followup disclosed that this access procedure was implemented in August 1984. Programmers, however, still have uncontrolled access to production programs. NFC's security officer told us that NFC believes uncontrolled access is needed to effectively deal with problems arising from unexpected interruptions in data processing. However, he acknowledged that NFC could establish a workable access control procedure to allow programmers controlled access to production programs only at times when circumstances warranted. In commenting on a draft of this report, the Assistant Secretary for Administration stated that further programmer access restrictions are tentatively scheduled for implementation in September 1985.

CONCLUSIONS

Stronger ADP controls are essential at NFC because of both the large volume of personnel and financial transactions processed annually and the requirements of the Federal Managers' Financial Integrity Act of 1982. Without adequate controls, these transactions and associated data files are vulnerable to unauthorized manipulation or destruction. In addition, this exposure could result in financial losses to the government and violations of the Privacy Act of 1974 if confidential personnel information is disclosed without authorization.

Steps have been taken or are planned by NFC to address our concerns, but all the necessary actions have not yet been completed. We believe that top management emphasis by both NFC and USDA will be needed to ensure that actions to resolve our concerns are completed and implemented.

RECOMMENDATIONS TO THE SECRETARY OF AGRICULTURE

We recommend that you direct the National Finance Center Director to report quarterly to the Assistant Secretary for Administration on the status of efforts to develop and implement

--contingency plans consistent with OMB Circular A-71 and FPMR 101-35.3 requirements and FIPS guidelines to ensure prompt recovery and restoration of NFC operations in case of a disaster or other unexpected events;

--program documentation standards and procedures consistent with FIPS guidelines;

--a system certification schedule for all NFC systems, consistent with OMB Circular A-71, which would include review of the adequacy of program documentation;

--independent testing standards and procedures for both program changes and new programs; and

--procedures that would allow programmers access to production programs only when circumstances warrant and on a controlled basis.

Agency Comments

In commenting on our draft report, Agriculture indicated that corrective action has been taken or planned on all of our findings. The only area of apparent disagreement is on the level of reporting on the status of NFC's corrective actions. Agriculture stated that the Director of the Office of Finance and Management will review quarterly reports on all open corrective actions, their status, and justifications for revised completion dates. However, because some other government agencies are or plan to begin using NFC for payroll and other payment services, we believe the status reports should be directed to the Assistant Secretary for Administration. In our view, the Assistant Secretary would be in a better position to judge the progress of corrective actions in relation to the increasing responsiblities entailed in providing services to other agencies. Agriculture's detailed comments are in enclosure I.

- - - - -

As you know, 31 U.S.C. 720 requires the head of a federal agency to submit a written statement on actions taken on our recommendations to the Senate Committee on Governmental Affairs and House Committee on Government Operations within 60 days of the report date and to the House and Senate Committees on Appropriations with the agency's first request for appropriations made over 60 days after the date of the report.

We are sending copies of this report to the Director of the Office of Management and Budget and the Chairmen of the Senate and House Committees on Appropriations, the Senate Committee on Governmental Affairs and the House Committee on Government Operations.

We appreciate the courtesy and cooperation extended by NFC officials to our representatives during this review.

Sincerely yours,

Frederick D. Wolf
Director

Enclosure

(931146)

DEPARTMENT OF AGRICULTURE
OFFICE OF THE SECRETARY
WASHINGTON, D. C. 20250

MAY 14 1985

Mr. J. Dexter Peach, Director
Resources, Community and Economic
Development Division
General Accounting Office
Washington, D.C. 20548

Dear Mr. Peach:

We are submitting our comments on the draft report entitled "Improvements Needed in General Automated Data Processing Controls at the National Finance Center."

> Recommendation: That the National Finance Center Director report quarterly to the Assistant Secretary for Administration on the status of efforts to develop and implement various corrective measures.

These actions are currently being tracked. The Director of the Office of Finance and Management has management responsibility for the National Finance Center, and will review quarterly reports on all open corrective actions, their status, and justifications for revised completion dates.

> Recommendation: Develop and implement contingency plans consistent with OMB Circular A-71 and FPMR 101-35.3 requirements and FIPS guidelines to ensure prompt recovery and restoration of NFC operations in case of a disaster or other unexpected events.

A contractor was employed to assist in developing a contingency plan to provide processing of 4 to 6 weeks for critical systems following a disruption. We have been testing the plan by various methods including actual recoverability exercises for the different critical systems. We have developed minimum hardware configuration requirements, constraints, and test period requirements. These tests and studies enable us to update the contractor's plan to better suit our operations.

We are in the process of developing specifications in order to obtain a Recovery Operating Center (back-up site). Considering the various aspects of the procurement process, it will be at least one year before a contract for the back-up site is secured. We will then be able to perform our first test at the Recovery Operating Center.

Recommendation: Develop and implement program documentation standards and procedures consistent with FIPS guidelines.

The program maintenance documentation packages, programs, and associated problems noted by GAO were reviewed and corrected by the programmers and supervisory personnel. Additionally, an independent group determined that the proper corrections were made and that the "dead" code was removed from programs.

The importance of documentation has been explained to NFC staff. All programmers are aware of this concern and that the Management Control Division is now routinely reviewing programmers' compliance with documentation standards.

The draft report stated that NFC's program maintenance package standard did not comply with FIPS PUB 38 and the law in the areas of: control totals, job control instructions, interface descriptions, and documentation of sensitive data and Privacy Act requirements. The NFC standard does require a description of control totals unless control totals are not needed (optional). For example, some generated reports such as personnel rosters do not require control totals. Since it appears that some confusion exists, we will update the standard to clarify the meaning of "optional" as related to control totals.

In the current computer environment, job control instructions are not run by individual programs but by system processes. The job control instructions by system processes are recorded on magnetic disk storage and are accessed by maintenance programmers through CRTs. Because maintenance programmers have access to the job control instructions through stored and various EDP devices, we believe the FIPS PUB 38 guideline which suggests that job instructions should be kept in each program maintenance manual is not applicable to our state-of-the-art environment.

Although the documentation standard does not use the word "interface," it does require interface descriptions. The standard requires a description of inputs including source of the input, a description of outputs including destination of the outputs, and an input-output chart depicting the flow of data to and from the program. We believe the standard meets the intent of FIPS PUB 38 guidelines in relation to interface descriptions. However, in updating the standard, we will more clearly specify that interface is synonymous with input/output.

In April of 1985, OFM prepared a draft Security Requirements Standard which addresses documentation of sensitive and Privacy Act data. The standard should be implemented by July 1985.

We believe the standards and procedures are generally consistent with the intent of FIPS guidelines. In those few areas where there are differences, adequate substitute procedures are being instituted. Departmental Regulation 3120-1 states that "Use of all FIPS guidelines is encouraged where applicable unless a substitute guideline is implemented...."

Recommendation: Develop and implement a system certification schedule for all NFC systems, consistent with OMB Circular A-71, which would include review of the adequacy of program documentation.

A schedule for certifying the payroll/personnel system was prepared, and we anticipate meeting the estimated completion date of August 30, 1985. Of the nine certification reviews scheduled, seven are completed and the other two were in process as of April 15, 1985.

A schedule for certifying all systems has been developed. Implementation of this schedule will begin upon completion of the certification of the Payroll/Personnel System.

Recommendation: Develop and implement independent testing standards and procedures for both program changes and new programs.

In February 1985, a methodology was developed for application software testing. The proposed methodology is being studied by various concerned groups. This methodology include rigorous procedures for:

- Software testing procedures
- Program change controls
- Division Chiefs' approvals on changes for critical or sensitive systems

Implementation of the final application testing procedure should be accomplished by July 1985.

Recommendation: Develop and implement procedures that would allow programmers access to production programs only when circumstances warrant and on a controlled basis.

Our procedures allow programmers to read, but not to write to, production programs. As GAO was informed, we plan to restrict the read access. We are also in the process of determining individual access requirements. However, additional activities by the programmers and some rearranging of program libraries are needed before programmers are completely restricted from accessing program source code. Implementation of this restriction is tentatively scheduled for September 1985.

We appreciate the opportunity to comment on the draft report.

Sincerely,

JOHN J. FRANKE, JR.
Assistant Secretary
for Administration

(931146)

31661