U.S. Department of Agriculture

Office of Inspector General
Financial & IT Operations

Audit Report

Purchase Card Management System Controls Need Strengthening

Report No. 11099-44-FM
August 2005

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

September 2, 2005

REPLY TO
ATTN OF: 11099-44-FM

TO: Russ Ashworth
Chief
Office of Procurement and Policy Management

Patricia E. Healy
Acting Chief Financial Officer
Office of the Chief Financial Officer

THROUGH: Arthur Goldman
Audit Liaison Officer
Departmental Administration

Kathy Donaldson
Audit Liaison Officer
Office of the Chief Financial Officer

FROM: Robert W. Young /s/
Assistant Inspector General
for Audit

SUBJECT: Purchase Card Management System Controls Need Strengthening

This report presents the results of our audit of controls over the Purchase Card Management System (PCMS). The Chief, Office of Procurement and Policy Management (OPPM) and Office of the Chief Financial Officer's response to the official draft, received on July 22, 2005, is included in its entirety as exhibit A. The Office of Inspector General's position is incorporated into the findings and recommendations section of the report.

Based on the information contained in the response, we concur with management decision on Recommendations 2 and 3 of the report. Although management's comments concerning the remaining recommendations, with the exception of Recommendations 1 and 4, adequately address required corrective action, management did not provide specific dates to complete planned actions. Management's comments to Recommendation 1 were not adequate because OPPM did not agree that it is its responsibility to ensure internal controls are in place and operating effectively.

In accordance with Departmental Regulation 1720-1, please furnish a reply within 60 days describing the corrective action taken or planned, including applicable timeframes, on our recommendations. Please note that the regulations require a management decision to be reached on all findings and recommendations within a maximum of 6 months from report issuance.

We appreciate the courtesies and cooperation extended to us during the audit.

Executive Summary

Purchase Card Management System Controls Need Strengthening

Results in Brief

Generally, we found that the transactions reviewed were proper and that the program met its intent of providing a cost beneficial process for procuring goods and services within the Department. However certain program controls could be strengthened to identify improper payments and potentially fraudulent activities. Specifically, we found that some cardholders failed to reconcile their transactions in the Purchase Card Management System (PCMS), the alert system could be made more effective, and policies governing supervisory oversight needed strengthening. These weaknesses occurred because there were limited controls in place to ensure that cardholders reconciled their purchases, oversight personnel indicated that they were overwhelmed by excessive messages in the alert system, and limited controls existed within the system to ensure that supervisors reviewed the appropriateness of cardholder purchases. As a result, potential improper transactions may not be detected, and agencies are at an increased risk of monetary losses resulting from undetected fraudulent, wasteful, or abusive purchase card transactions.

The Office of the Chief Financial Officer (OCFO) and the Office of Procurement and Property Management (OPPM) could implement additional controls to ensure the integrity and security of the PCMS system and improve its reliability and effectiveness in preventing potential improper payments. We found (1) users with unrestricted and unmonitored administrative access to the PCMS database, (2) password settings did not conform with Federal requirements, (3) budget object classification codes (BOCC) were not verified, (4) transactions posted to cancelled cards, (5) incorrect or missing cardholder data, and (6) unverified lender rebates. OCFO was aware that many of these weaknesses existed; however, it had not implemented corrective actions due to other priorities. As a result, the PCMS is at greater risk of unauthorized access and improper purchases. Further, the Department may not be receiving the appropriate rebate from the lender in accordance with its contract. Specifically:

- We found that 14 users had unrestricted and unmonitored database administrator privileges to PCMS data, access to PCMS was not documented, passwords were not encrypted, and password settings were not configured in accordance with departmental and Federal guidelines. In addition, the PCMS application did not force users to change their initial password.

- PCMS did not enter the appropriate BOCC.

- There was no internal control to prevent a cardholder (whether a current or separated employee) from making charges on an account after the account had been cancelled.

- Purchase cards were not cancelled in a timely manner after the cardholder separated from the agency. OCFO removed separated employees' access to the PCMS application on a monthly basis, but no prescribed controls existed to ensure that those employees' purchase cards were cancelled.

- We identified 126 cardholders whose social security numbers (SSN) in PCMS were invalid or associated with an incorrect individual.

- The Department earns a rebate from the lender based on the volume of purchase card transactions and payments made. In fiscal year 2003, the lender paid the Department over $4.4 million in rebates related to purchase card transactions. We found that OCFO ensured that the rebate planned by the lender was actually received, but it had not independently verified that the lender calculated the rebate accurately.

Recommendations In Brief

We recommended the following to strengthen internal controls and to prevent and detect improper payments made under the Purchase Card Program:

- OPPM should establish controls to enforce its policies to (1) address alert messages within 30 days of receipt and (2) reconcile and review purchase card transactions on a monthly basis.

- OPPM in coordination with OCFO should modify PCMS to (1) automatically suspend purchase cards that have unreconciled transactions greater than 60 days and (2) prohibit cardholders from modifying alert messages for potentially suspicious transactions.

- OCFO should validate whether database administrator access is needed for all 14 users we identified to perform their job functions. Remove or restrict access as needed and establish procedures and controls limiting future designation.

- OCFO should modify PCMS and the Security Access Management System (SAMS), as appropriate, to ensure that user password controls conform to departmental and Federal guidelines.

- OPPM in coordination with OCFO should establish controls to require users to validate the accuracy of the BOCC for each transaction.

- OPPM in coordination with OCFO should modify the PCMS to (1) reject transactions from the lender associated with cards that have been cancelled, (2) establish an edit to check the validity of cardholder's SSN, (3) direct the lender to cancel a card at the same time that PCMS drops a cardholder's system access, and (4) independently calculate and verify that the appropriate rebate was received.

Agency Response

OCFO and OPPM generally agreed with the findings and recommendations, except for Recommendations 1 and 4. With respect to Recommendation 1, OPPM did not agree that it shared responsibility with the user agencies to implement adequate effective internal controls to enforce policies to (1) reconcile transactions and address alert messages in a timely manner and (2) review transactions on a monthly basis. With respect to Recommendation 4, management indicated that Oracle does not store pass words in clear text.

OIG Position

We continue to believe that OPPM shares responsibility with user agencies to help ensure internal controls are in place and operating effectively. The lack of effective internal controls within PCMS is evidenced by over 1,400 cardholders not reconciling approximately 6,700 transactions totaling over $3.4 million, within 30 days.

We agree that Oracle encrypts passwords; however, PCMS passwords are stored in clear text in SAMS which is an IBM system used to access the Oracle based PCMS.

Abbreviations Used in This Report

ACFO-FS	Associate Chief Financial Officer-Financial Systems
APC	Agency Program Coordinator
BOCC	Budget Object Classification Code
CCB	Change Control Board
DR	Departmental Regulation
IRMD	Information Resources Management Division
ISSO	Information System Security Office
LAPC	Local Agency Program Coordinator
NFC	National Finance Center
NIST	National Institute of Standards and Technology
OCFO	Office of the Chief Financial Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPPM	Office of Procurement and Property Management
PCMS	Purchase Card Management System
SSN	Social Security Number
USDA	U.S. Department of Agriculture

Table of Contents

Background and Objectives

Background

The U.S. Department of Agriculture's (USDA) Purchase Card Program is part of a Government-wide initiative to streamline the Federal agency acquisition processes. The program provides agencies with a low-cost and efficient vehicle to make small purchases of $2,500 or less directly from vendors. Agencies and vendors benefit from the program through lower processing costs and reduced complexity from traditional procurement methods. In fiscal year 2003, USDA agencies made over $570 million in purchases using the Purchase Card Program.

The Purchase Card Program uses a VISA credit card issued by a commercial lender, similar to a personal credit card. Purchase cards are marked with the United States of America seal and the words "For Official U.S. Government Purchases Only" to distinguish them from a personal credit card. Also, some cardholders are issued convenience checks tied to the credit account that can be used for purchases from merchants that do not accept credit cards.[1]

The Purchase Card Management System (PCMS) is an automated reconciliation and payment system that assists the users and management in monitoring expenses. PCMS is a Windows-based system used to track, reconcile, and control purchases made with purchase cards. On a daily basis, the lender downloads purchase card transaction data and purchase card master data to the Office of the Chief Financial Officer (OCFO). OCFO makes payments to the lender for purchases billed according to a scheduled billing cycle.

The Office of Procurement and Property Management (OPPM) has overall responsibility for managing the USDA Purchase Card Program and overseeing the development and maintenance of PCMS. Each agency within USDA has an Agency Program Coordinator (APC) who is responsible for the overall program in that agency, and acts as the agency's contact with OPPM and the lender. For geographically dispersed agencies, Local Agency Program Coordinators (LAPC) are responsible for the day-to-day operations of the Purchase Card Program in their designated area. The LAPC is appointed by the head of the contracting office, subject to the concurrence of the APC. Agency APC and LAPC responsibilities include cardholder training, purchase card record maintenance, oversight of purchase card transactions, and cancellation or activation of cardholder accounts. Agency management determines who in their organizations should receive purchase cards and convenience checks and recommends the monthly purchase limits.

[1] As of July 1, 2003, the use of convenience checks was limited in an effort to minimize misuse. Agencies are still permitted to use convenience checks in certain situations.

Ultimately, cardholders and their supervisors remain responsible for reviewing purchases to ensure that they are necessary and proper.

Objectives

Our audit objective was to determine if improper purchases were being made using Government purchase cards or convenience checks. Also, we evaluated controls within PCMS to detect and prevent monetary losses from fraudulent, wasteful, or abusive purchase card transactions.

Findings and Recommendations

Section 1. Purchase Card Program Oversight

Finding 1 Additional Oversight Could Improve Purchase Card Program Effectiveness

Generally, we found that the transactions reviewed were proper and that the program met its intent of providing a cost beneficial process for procuring goods and services within the Department. However certain program controls could be strengthened to identify improper payments and potentially fraudulent activities. Specifically, we found that some cardholders failed to reconcile their transactions in PCMS, the alert system could be made more effective, and policies governing supervisory oversight needed strengthening. These weaknesses occurred because there were limited controls in place to ensure that cardholders reconciled their purchases, the alert system overwhelmed oversight personnel with excessive messages, and limited controls existed within the system to ensure that supervisors reviewed the appropriateness of cardholder purchases. As a result, potential improper transactions may not be detected, and agencies are at an increased risk of monetary losses resulting from undetected fraudulent, wasteful, or abusive purchase card transactions.

Unreconciled Transactions

We noted that over 1,400 cardholders had not reconciled approximately 6,700 transactions totaling over $3.4 million within 30 days as required by departmental regulations (DR). We also noted agency managers had not suspended (deactivated) 685 cardholders’ accounts after they had not reconciled over 3,000 transactions totaling about $750,000 within the 60-day time limit.[2] This occurred because agency managers did not take action to monitor or restrict the purchasing activity of cardholders who failed to timely reconcile their transactions. As a result, fraudulent or improper transactions may go undetected and not disputed through the lender. Furthermore, the cardholder’s agency may have no recourse in resolving fraudulent or improper transactions.

DR 5013-6 states that cardholders shall reconcile their accounts no longer than 30 days after a transaction appears in PCMS, absent extenuating

[2] DR 5013-6, “Use of the Purchase Card and Convenience Check,” dated February 13, 2003, requires cardholders to reconcile their accounts no longer than 30 days after a transaction appears in PCMS, absent extenuating circumstances. Further, program coordinators shall deactivate the account of any cardholder who fails to reconcile transactions within 60 days after each transaction appears in PCMS. Furthermore, transactions cannot be disputed after 60 days.

circumstances. Further, program coordinators shall deactivate the account of any cardholder who fails to reconcile transactions within 60 days after each transaction appears in PCMS.

The PCMS Cardholder Responsibilities Guide requires that the cardholder contact the merchant to resolve any dispute before processing it through PCMS. If the dispute cannot be resolved with the merchant, the cardholder must mark the transaction as a disputed transaction in PCMS and fax the lender notice that the transaction is in dispute. The cardholder has 60 days from the date of a transaction to file a dispute with the lender. After the 60-day time limit, the lender is not obligated to accept any disputes of questioned transactions. Further, the guide requires the cardholder to reconcile transactions at least once a month in PCMS using documentation retained from each purchase. Cardholders who frequently use their purchase cards should increase the frequency of reconciliation in order to keep reconciliation sessions brief and to assist agency management and finance officials in monitoring the status of funds.

Alert Message System Could be Improved

PCMS automatically creates alert messages when a purchase meets certain criteria such as suspicious merchant category codes (e.g., pawn shops, liquor stores, jewelry stores, camera stores, etc.), potential split transactions, unreconciled transactions after 30 days, and transactions on closed accounts. However, because of the volume of alert messages, agency oversight personnel have not been vigilant in monitoring those alerts. Agency coordinators cited difficulty in using the system and excessive workload as reasons for not keeping current in reading and acting on alert messages.

We also found that all alert messages are sent to the responsible purchase cardholder, LAPC, and APC rather than to specific individuals identified in the system requirements document. PCMS requirements documentation requires that alerts for suspicious transactions should go to LAPCs and not to responsible purchase cardholders. OPPM could not provide a reasonable answer as to why the alert message system within PCMS did not match the system's requirements. The current distribution of alert messages diminishes the effectiveness of the internal control because cardholders are alerted when the system identifies certain transactions intended for review by agency oversight personnel. For example, an alert that a purchase was made from a vendor with a suspicious merchant category code could be seen by the cardholder that perpetrated the improper purchase. The cardholder could conceal an improper payment by marking the alert message as "read."[3]

[3] Because of the volume of alert messages received, oversight personnel generally ignore messages marked as "read" assuming that appropriate action had been taken.

Lack of Supervisory Review of Transactions

OPPM established a policy that cardholders' supervisors should review their employees' purchase card transactions on a quarterly basis. However, we noted that this policy was not enforced at the four agencies we reviewed to assure that these reviews were actually being completed. In addition, while one agency implemented a supervisory review requirement of this process, it was ineffective. The LAPC at that agency sent monthly reports of cardholder transactions to the supervisors; however, no documentation was ever returned to the LAPC from the supervisor to assure that the review was actually completed. The other three agencies did not send a list of transactions to cardholder supervisors, and the personnel had no means to assure that supervisors had actually reviewed purchase card transactions. More improper purchases could be detected or deterred if a formal supervisory program was established to review transactions on a monthly rather than quarterly basis. This would allow the agency to timely dispute charges with the lender within the 60-day timeframe.

Recommendation No. 1

OPPM should establish controls to enforce its policies to (1) reconcile transactions and address alert messages within 30 days of receipt and (2) review purchase card transactions on a monthly basis.

Agency Response. OPPM did not concur. It stated that the recommendation is misdirected. The Office of Inspector General (OIG) should direct this recommendation to the heads of agencies whose purchase card programs were reviewed during the audit. OPPM has taken a number of actions to improve the performance of APCs and LAPCs over the years, including the promulgation of an internal control blueprint in 2003. OPPM will continue to encourage agencies to improve reconciliations rates and to address alert messages. However, agencies also must be responsible for deficiencies in their purchase card programs. APCs and LAPCs work for their own agencies; they are not OPPM employees. OPPM does not propose to take the corrective action recommended.

OIG Position. We continue to believe that OPPM shares responsibility with user agencies to help ensure internal controls are in place and operating effectively. The lack of effective internal controls within PCMS is evidenced by over 1,400 cardholders not reconciling approximately 6,700 transactions totaling over $3.4 million, within 30 days.

OPPM should analyze potential systemic controls that could be implemented within the PCMS application that would prompt compliance by agency cardholders that habitually do not reconcile and review transactions in a timely manner (e.g., suspend and/or cancel the account).

Recommendation No. 2

OPPM in coordination with OCFO should modify PCMS to (1) automatically suspend purchase cards that have unreconciled transactions greater than 60 days and (2) prohibit cardholders from modifying alert messages for potentially suspicious transactions.

Agency Response. OPPM concurred with both parts of the recommendation. (1) The Procurement Policy Division prepared a change request to automatically suspend purchase cards that have unreconciled transactions greater than 60 days. A change request modification document was created and submitted to OCFO Change Control Board (CCB) to address the recommendation. The change request is currently under review and analysis to determine the appropriate corrective action to satisfy the specific recommendation. The requested modification will be implemented in 2006. (2) The change request to prohibit cardholders from modifying alert messages for potentially suspicious transactions was included in PCMS Release 5.1, implemented in March 2005.

OIG Position. We concur with the management decision.

Finding 2 Purchase Card Management System Controls Need Strengthening

OCFO and OPPM should implement additional controls to ensure the integrity and security of the PCMS system and improve its reliability and effectiveness in preventing potential improper payments. We found (1) users with unrestricted and unmonitored administrative access to the PCMS database, (2) password settings did not conform with Federal requirements, (3) budget object classification codes were not verified, (4) transactions posted to cancelled cards, (5) incorrect or missing cardholder data, and (6) unverified lender rebates. OCFO was aware that many of these weaknesses existed; however, it had not implemented corrective actions due to other priorities. As a result, the PCMS system is at greater risk of unauthorized access and improper purchases. Further, the Department may not be receiving the appropriate rebate from the lender in accordance with its contract. Details follow.

Access Controls to PCMS Data

We found that 14 users had unrestricted and unmonitored database administrator privileges to PCMS data, access to PCMS was not documented, passwords were not encrypted, and password settings were not configured in accordance with departmental and Federal guidelines. As a result, PCMS data is at risk of compromise from unauthorized access.

OMB established a minimum set of controls for agencies' automated information security programs.[4] Agencies are required to establish controls to assure adequate security for all information processed, transmitted, or stored. The National Institute of Standards and Technology (NIST) further specifies management, operational, and technical controls.[5] It illustrates the benefits of security controls and the major techniques or approaches for each control. Both NIST and OMB advocate implementation of the "least privilege" concept, granting users only the access required to perform their duties.

We identified 14 users from several divisions of OCFO/National Finance Center (NFC) that had database administrative authority over PCMS data that

[4] OMB Circular A-130, Appendix III, "Security of Federal Automated Information Resources," dated November 28, 2000.
[5] NIST Special Publication 800-12, "An Introduction to Computer Security: The NIST Handbook," dated October 1995.

was not restricted to the authority needed to perform their duties as required by NIST Special Publication 800-14, "Generally Accepted Principles and Practices for Securing Information Technology Systems." Administrative authority is the highest level of access to a database and allows those users to add, modify, or delete data. For example, we identified three users from the security staff that establish new user accounts. Instead of limiting their authority to only establish user identifications, they were given full administrative authority to the full PCMS database. In addition, there was no tracking system to identify the activity processed by these users. Therefore, we were unable to determine whether inappropriate actions had occurred.

We also found that users' passwords were stored in clear text and not encrypted in the Security Access Management, contrary to NIST Special Publication 800-14.[6] In addition, the PCMS application did not force users to change their initial password as required by Department Manual 3140-001, "Management ADP Security Manual." OCFO was aware of these password control weaknesses but could not explain why the system had been designed with these weaknesses, or when they would be corrected.

Budget Object Classification Code

PCMS does not contain a provision to allow for the appropriate budget object classification code (BOCC) to be entered. This code is critical within the Department's accounting applications to ensure that tax forms required by the Internal Revenue Service are properly prepared and sent to vendors. PCMS was designed to enter a default BOCC regardless of the type of purchase. Cardholders are subsequently responsible for changing it, if necessary. OCFO was aware of the problem and has requested a change through its application change control board; however, at the time of our review, the change had not been approved.

Charges Occurred on Cancelled Cards

There was no internal control to prevent a cardholder (whether a current or separated employee) from making charges on an account after the account had been cancelled. PCMS does not perform an edit check to determine if a transaction transferred from the lender is associated with a deactivated card. The lender stated that it is standard industry practice to honor certain recurring charges despite the card being cancelled. The lender also stated that it is the cardholder's or APC's responsibility to make alternate financial arrangements for recurring transactions associated with a cancelled card.

[6] SAMS is an IBM system used to access PCMS.

Cards Not Cancelled After Cardholder Separated

Purchase cards were not cancelled in a timely manner after the cardholder separated from the agency. OCFO/NFC removed separated employees' access to the PCMS application on a monthly basis, but no prescribed controls were in place to ensure that those employees' purchase cards were cancelled. As a result, ex-employees could potentially continue to make purchases on the credit card.

OCFO/NFC systems security staff informed us that they run a report once a month that compares the social security numbers (SSN) of purchase cardholders with the Department's employee database. The security staff uses this report to identify PCMS users who had left the Department and no longer needed access to PCMS. However, the security staff does not cancel the purchase card, rather, per DR 5013-6, LAPC's are required to cancel cards. We found that no control provision had been set forth to assure this action is taken in a timely manner. PCMS could be modified to direct the lender to cancel a card at the same time OCFO/NFC cancels the PCMS system access.

Invalid Social Security Numbers

We identified 126 cardholders whose SSNs in PCMS were invalid or associated with an incorrect individual. This occurred because PCMS was not programmed with a routine to ensure that only valid SSNs were entered into the system for each cardholder. As a result, there is an increased risk that unauthorized personnel may obtain and use purchase cards.

We also performed a comparison of SSNs between PCMS and the Department's personnel system to determine whether all cardholders were current employees of USDA. Our analysis for the four agencies identified SSNs that were in PCMS but not in the personnel system. This occurred because the PCMS cardholder table was not validated against the Department's personnel database. Ultimately, we were able to find the correct SSNs by performing a name and agency search on the personnel database.

The PCMS lead developer informed us that a change request was approved to have every SSN in the PCMS cardholder table validated against the Department's personnel database. Further, newly established purchase card users would have to be validated against the Department's personnel database before a card would be issued.

Lack of Rebate Calculation

The Department earns a rebate from the lender based on the volume of purchase card transactions and payments made. In fiscal year 2003, the lender paid the Department over $4.4 million in rebates related to purchase card transactions. We found that OCFO ensured that the rebate planned by the lender was actually received, but it had not independently verified that the lender calculated the rebate accurately. At one time, PCMS lacked sufficient data to determine the payments; therefore, an independent calculation of the estimated rebate was not possible. However, the current version of PCMS now contains the necessary fields to validate the rebate estimate. To ensure the Department receives its rightful rebate, PCMS should be updated to calculate and verify that the appropriate rebate was received from the lender.

Recommendation No. 3

OCFO should validate whether full database administrator access is needed for all 14 users we identified to perform their job functions. Remove or restrict access as needed and establish procedures and controls limiting future designation.

Agency Response. OCFO/National Finance Center's, Information Resources Management Division (IRMD) performed an analysis and review of the 14 users identified in the audit having database administrative authority over PCMS data. The goal to validate needed database authority over PCMS data resulted in the establishment of access to only those employees who require the access to perform their regular duties. Of the 14 users identified, actions were taken to remove access for a duplicate user identification as requested by the Data Base Management Branch, NFC, and three were reclassified into unique roles for Security Administration limiting their authority to establish and update. The access of the remaining nine users was required in order to perform their regular job duties.

The OCFO/NFC's Information System Security Office (ISSO) is currently designing and implementing reports using a new logging tool implemented to log and monitor all Web and Unix servers attached to the NFC network. Currently, daily Oracle reports are generated listing users with Data Base Administrator authority and the status (successful only) of approximately 18 Oracle commands. Additional reports are planned to include more activities like administrator activity, violations, inactive accounts, etc.

NFC role owners and ISSO are working together to implement role-based access and produce reports for management review of access and roles of their staff. Role based access and monitoring has been established for IRMD employees. Associate Chief Financial Officer-Financial Systems

(ACFO-FS) and ISSO will work together to implement role based security control monitoring for other OCFO employees by September 30, 2006.

Access privileges were reviewed, corrected and finalized in May 2005. ISSO's plan for role base security control monitoring and reporting on implementation for ACFO-FS is scheduled for September 30, 2006.

OIG Position. We concur with the management decision.

Recommendation No. 4

OCFO should modify the PCMS application and SAMS, as appropriate, to ensure that user password controls conform to departmental and Federal guidelines.

Agency Response. The report states that user passwords are stored in clear text and unencrypted. This is untrue. The PCMS database is built on Oracle. Oracle password controls conform to departmental and Federal guidelines through encryption with a one-way hash algorithm before they are stored in the database. Other terms for this are message digest, digital signature, one-way encryption, digital fingerprint, or cryptographic hash. Oracle uses a Data Encryption Standard algorithm on passwords. What is stored is a hash or digested value and it is NOT reversible. It appears to be a string of hexadecimal characters and has a fixed length. If someone obtains this string or digest, they are unable to determine the password.

The PCMS application did not force users to change their initial password as required by Departmental Manual 3140-1. A change request is being created that addresses the PCMS access/sign-on process that will force users to change their initial password. Following the appropriate research and analysis on the change request, implementation of the requirement will be scheduled for release in FY 2006.

OIG Position. We agree that Oracle does not store passwords in clear text or unencrypted. However, PCMS passwords are stored in clear text in SAMS which is an IBM system used to access the Oracle based PCMS. As such, SAMS should be modified to encrypt passwords.

Recommendation No. 5

OPPM in coordination with OCFO should establish controls to require users to validate the accuracy of the BOCC for each transaction.

Agency Response. OPPM concurred in part. It indicated that there is no way to edit a BOCC during reconciliation to ensure that the BOCC accurately describes the product or service purchased. A change request was approved by the CCB and is currently under development. However, the statistical sampling feature in the alert function already allows LAPCs to review data reported for a transaction, including the BOCC reported by the cardholder. We understand OIG's concern about the present system's autofilling a default BOCC that the cardholder need not verify or change prior to approving/reconciling a transaction. Autofilling the BOCC field is required for system functionality. A change request to use a crosswalk between merchant category code and BOCC has been approved by the CCB, and work on development of the crosswalk has commenced. The crosswalk will autofill the BOCC field with a BOCC corresponding to the merchant category code reported by the bank. While this is not a total cure, it will substantially increase the accuracy of BOCCs reported in PCMS. No release date has been determined for this change.

OCFO and OPPM will include crosswalk functionality in the PCMS update, to be released by December 31, 2006.

OIG Position. We concur with the proposed corrective actions; however, the estimated completion date of December 31, 2006 is beyond the 1 year timeframe required by Departmental Regulation (DR) 1720-1. In order to achieve management decision, please provide detailed, time phased interim completion dates.

Recommendation No. 6

OPPM in coordination with OCFO should modify the PCMS to (1) reject transactions from the lender associated with cards that have been cancelled, (2) establish an edit to check the validity of cardholder's SSN, (3) direct the lender to cancel a card at the same time that PCMS drops a cardholder's system access, and (4) independently calculate and verify that the appropriate rebate was received.

Agency Response. OPPM's position on each numbered part of Recommendation 6 is as follows:

1. OPPM generally concurred that transactions against cancelled accounts should be declined by the lender or disputed by USDA if not declined. OPPM has an alert message in PCMS to notify LAPCs of transactions posted against cancelled accounts. OPPM and OCFO are modifying PCMS to automatically notify the bank when a cardholder separates from USDA. However, a certain period of time after separation must be allowed for trailing transactions; i.e., transactions made before a cardholder separates, but not posted until after the cardholder leaves USDA. Finally, the lender may not decline recurring transactions such

as renewals of magazine subscriptions. Rules governing credit card accounts stipulate that the subscriber must take some action to cancel the account or transaction to be honored.

2. OPPM concurred. OPPM and OCFO are working on validation of cardholder SSNs. The first phase will be review and validation of all SSNs reported for current cardholders. The second phase will be to install a SSN edit check for all new cardholder accounts. PCMS version 6.1, to be released in 2006, will validate an employee's SSN against the employee database whenever an account is created or modified.

3. OPPM concurred. OPPM and OCFO are modifying PCMS to notify the bank automatically when a cardholder separates from USDA. A change request approved for PCMS version 5.2, will automate a cancellation request when a cardholder user identification is dropped from PCMS.

4. OPPM concurred. An emergency change request was approved to calculate the refunds independently for comparison against the actual refund that is received from the lender. OPPM is discussing methods of rebate verification with OCFO and requirements are being developed.

OPPM anticipates that all modifications to PCMS will be completed by the 2006 release of PCMS version 6.2.

OIG Position.

We concur with the proposed corrective actions; however, the estimated completion date of 2006 is not specific and must be within the 1 year timeframe required by DR 1720-1. In order to achieve management decision, a specific completion date must be provided and if the date is beyond the 1 year requirement, please provide detailed, time phased interim completion dates.

Scope and Methodology

We performed our audit at the OCFO/NFC, located in New Orleans, Louisiana and at OPPM, and agency offices in Washington D.C. We selected transactions for the following four agencies based on the volume of activity:

- The Animal and Plant Health Inspection Service,
- Natural Resources Conservation Service,
- Agricultural Research Service,
- and the Food Safety and Inspection Service.

We conducted our review from December 2003 through September 2004.

To accomplish our objectives, we performed the following:

- Interviewed the agencies APCs to discuss their duties with the Purchase Card Program, oversight procedures, and questionable transactions.

- Reviewed OPPM and OCFO procedures and policies, and ongoing efforts designed to minimize and uncover improper purchase card transactions.

- Obtained relevant policy guidance documentation relating to the governance of the use of purchase cards (including the U.S. Government Accountability Office, Department, and OMB).

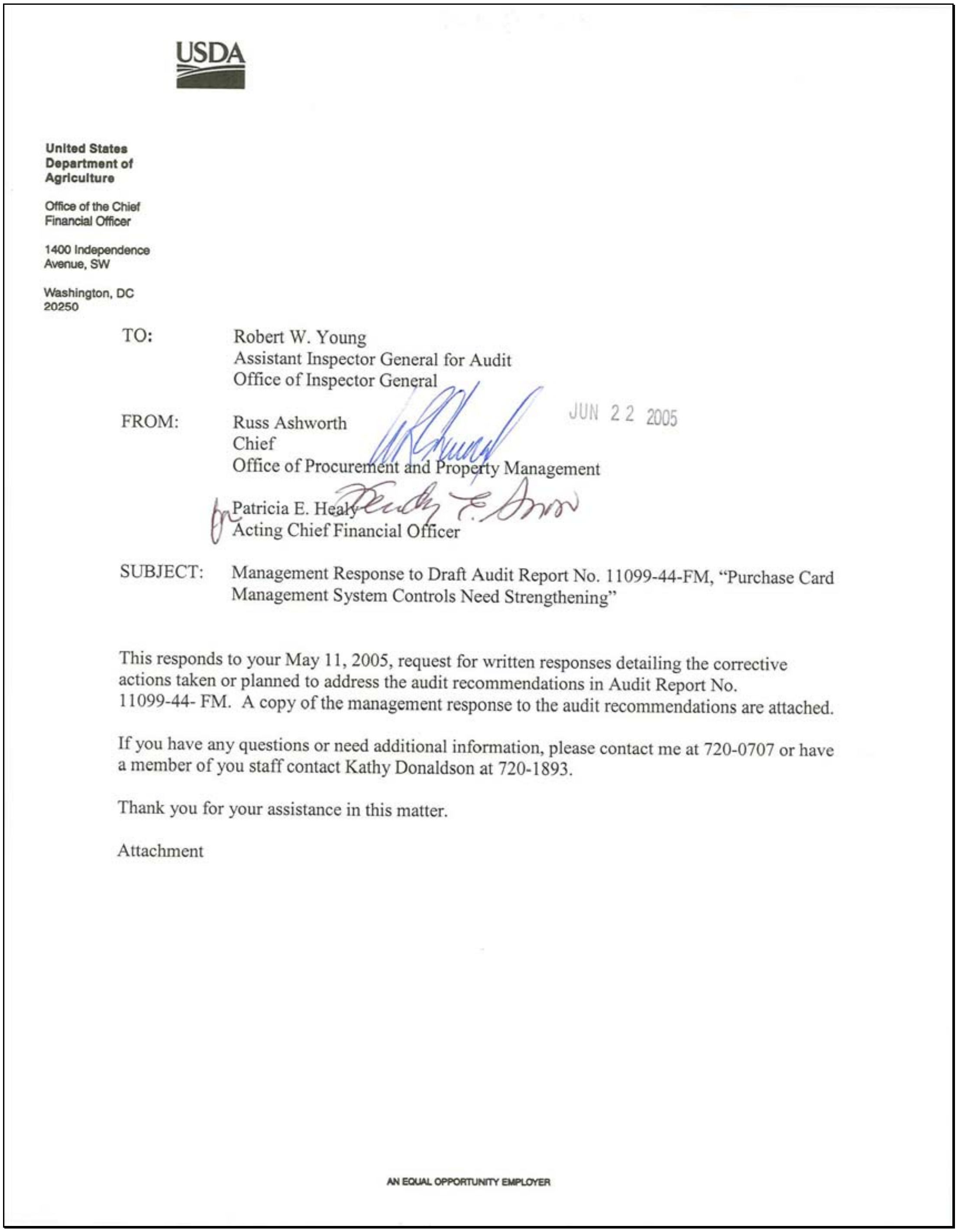
- Analyzed PCMS transactions and PCMS alert messages.

- Conducted various computer analyses of purchase card transaction activities within the PCMS database using commercially available analytical software to identify potential improper payments.

- Obtained supporting documentation for transactions, and evaluated the information provided for compliance with purchase card requirements.

We conducted this audit in accordance with “Government Auditing Standards.”

Exhibit A – Agency Response to the Draft Report



USDA

United States
Department of
Agriculture

Office of the Chief
Financial Officer

1400 Independence
Avenue, SW

Washington, DC
20250

TO: Robert W. Young
Assistant Inspector General for Audit
Office of Inspector General

FROM: Russ Ashworth
Chief
Office of Procurement and Property Management

JUN 22 2005

Patricia E. Healy
Acting Chief Financial Officer

SUBJECT: Management Response to Draft Audit Report No. 11099-44-FM, "Purchase Card Management System Controls Need Strengthening"

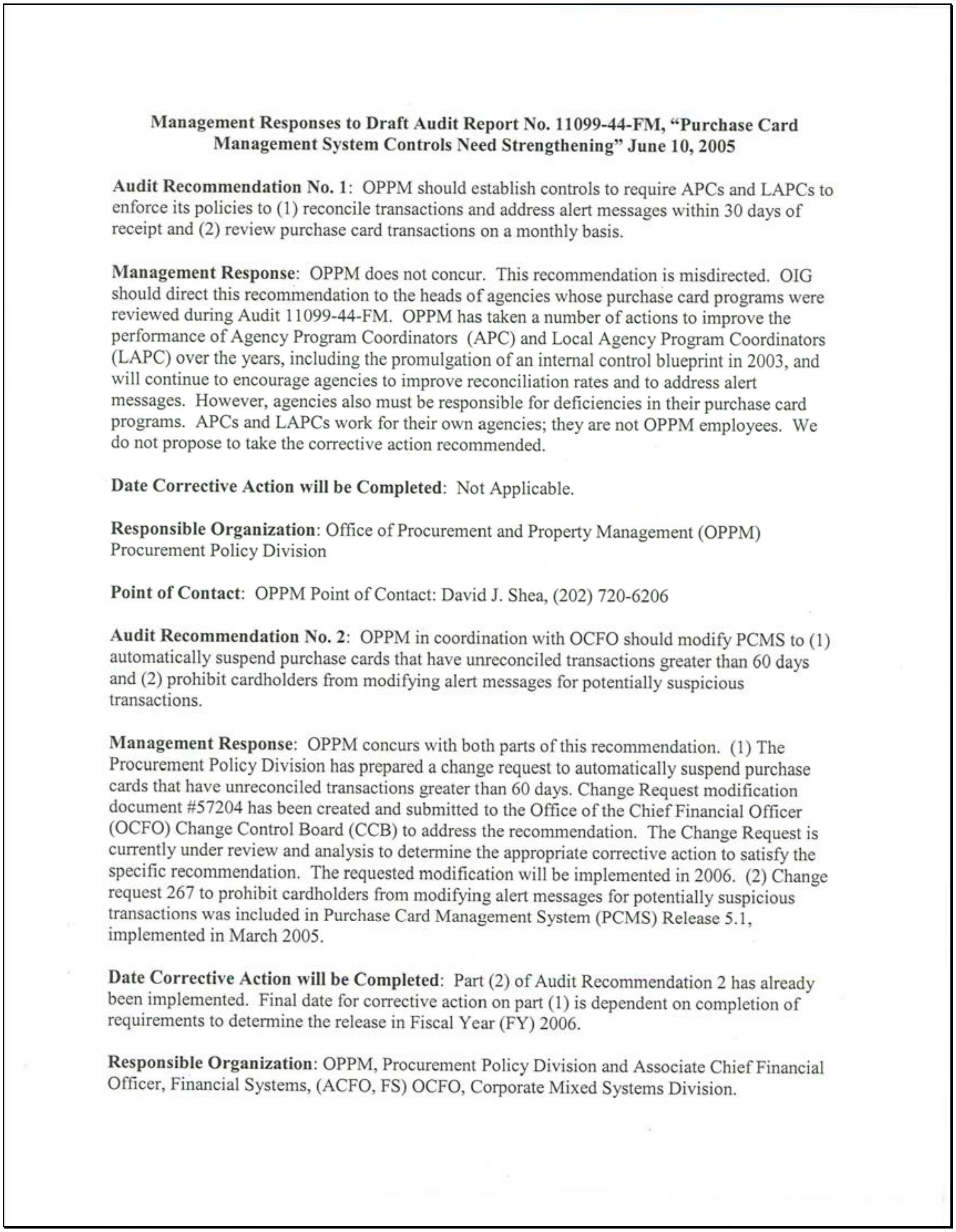
This responds to your May 11, 2005, request for written responses detailing the corrective actions taken or planned to address the audit recommendations in Audit Report No. 11099-44- FM. A copy of the management response to the audit recommendations are attached.

If you have any questions or need additional information, please contact me at 720-0707 or have a member of you staff contact Kathy Donaldson at 720-1893.

Thank you for your assistance in this matter.

Attachment

AN EQUAL OPPORTUNITY EMPLOYER



Management Responses to Draft Audit Report No. 11099-44-FM, "Purchase Card Management System Controls Need Strengthening" June 10, 2005

Audit Recommendation No. 1: OPPM should establish controls to require APCs and LAPCs to enforce its policies to (1) reconcile transactions and address alert messages within 30 days of receipt and (2) review purchase card transactions on a monthly basis.

Management Response: OPPM does not concur. This recommendation is misdirected. OIG should direct this recommendation to the heads of agencies whose purchase card programs were reviewed during Audit 11099-44-FM. OPPM has taken a number of actions to improve the performance of Agency Program Coordinators (APC) and Local Agency Program Coordinators (LAPC) over the years, including the promulgation of an internal control blueprint in 2003, and will continue to encourage agencies to improve reconciliation rates and to address alert messages. However, agencies also must be responsible for deficiencies in their purchase card programs. APCs and LAPCs work for their own agencies; they are not OPPM employees. We do not propose to take the corrective action recommended.

Date Corrective Action will be Completed: Not Applicable.

Responsible Organization: Office of Procurement and Property Management (OPPM) Procurement Policy Division

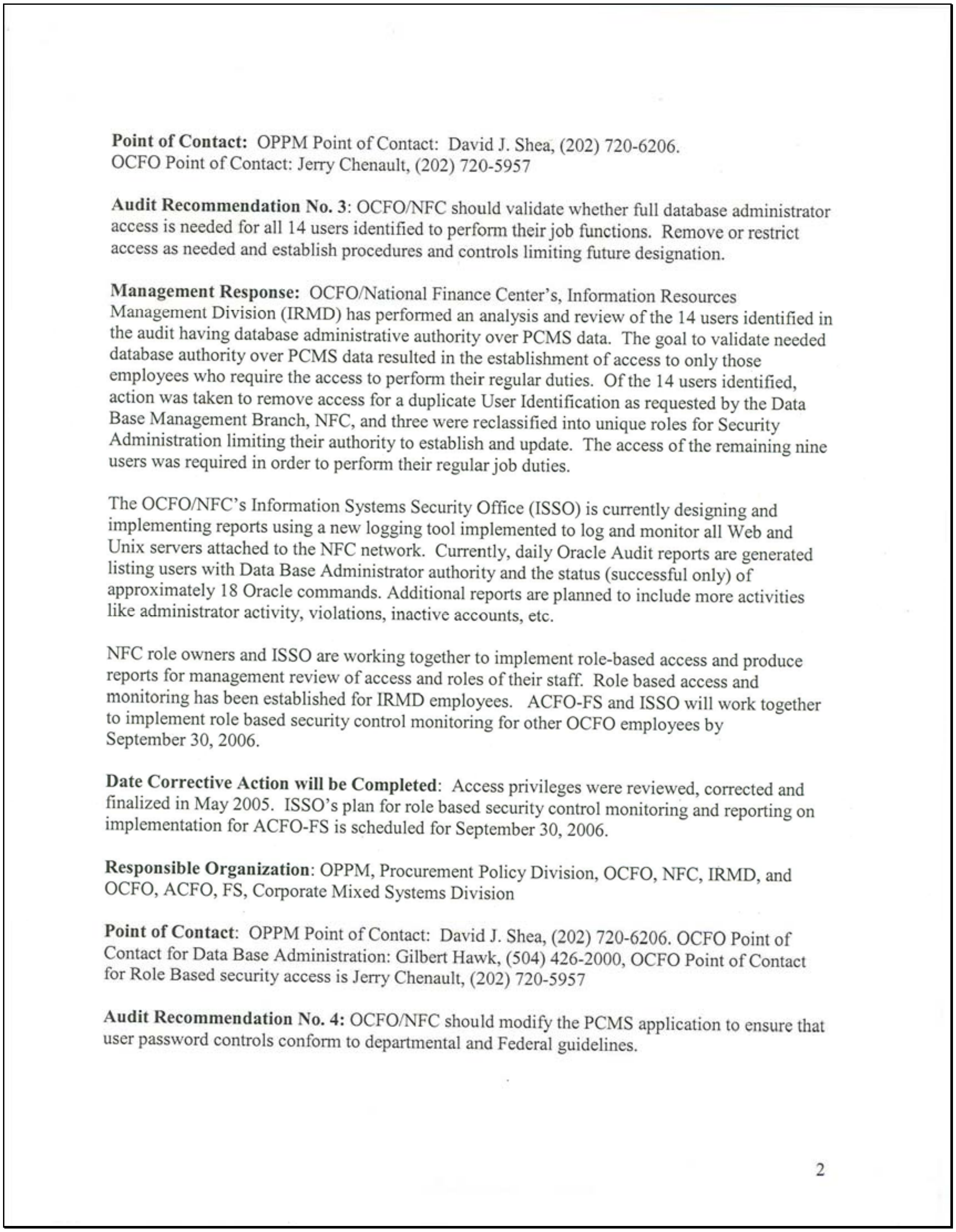
Point of Contact: OPPM Point of Contact: David J. Shea, (202) 720-6206

Audit Recommendation No. 2: OPPM in coordination with OCFO should modify PCMS to (1) automatically suspend purchase cards that have unreconciled transactions greater than 60 days and (2) prohibit cardholders from modifying alert messages for potentially suspicious transactions.

Management Response: OPPM concurs with both parts of this recommendation. (1) The Procurement Policy Division has prepared a change request to automatically suspend purchase cards that have unreconciled transactions greater than 60 days. Change Request modification document #57204 has been created and submitted to the Office of the Chief Financial Officer (OCFO) Change Control Board (CCB) to address the recommendation. The Change Request is currently under review and analysis to determine the appropriate corrective action to satisfy the specific recommendation. The requested modification will be implemented in 2006. (2) Change request 267 to prohibit cardholders from modifying alert messages for potentially suspicious transactions was included in Purchase Card Management System (PCMS) Release 5.1, implemented in March 2005.

Date Corrective Action will be Completed: Part (2) of Audit Recommendation 2 has already been implemented. Final date for corrective action on part (1) is dependent on completion of requirements to determine the release in Fiscal Year (FY) 2006.

Responsible Organization: OPPM, Procurement Policy Division and Associate Chief Financial Officer, Financial Systems, (ACFO, FS) OCFO, Corporate Mixed Systems Division.



Point of Contact: OPPM Point of Contact: David J. Shea, (202) 720-6206.
OCFO Point of Contact: Jerry Chenault, (202) 720-5957

Audit Recommendation No. 3: OCFO/NFC should validate whether full database administrator access is needed for all 14 users identified to perform their job functions. Remove or restrict access as needed and establish procedures and controls limiting future designation.

Management Response: OCFO/National Finance Center's, Information Resources Management Division (IRMD) has performed an analysis and review of the 14 users identified in the audit having database administrative authority over PCMS data. The goal to validate needed database authority over PCMS data resulted in the establishment of access to only those employees who require the access to perform their regular duties. Of the 14 users identified, action was taken to remove access for a duplicate User Identification as requested by the Data Base Management Branch, NFC, and three were reclassified into unique roles for Security Administration limiting their authority to establish and update. The access of the remaining nine users was required in order to perform their regular job duties.

The OCFO/NFC's Information Systems Security Office (ISSO) is currently designing and implementing reports using a new logging tool implemented to log and monitor all Web and Unix servers attached to the NFC network. Currently, daily Oracle Audit reports are generated listing users with Data Base Administrator authority and the status (successful only) of approximately 18 Oracle commands. Additional reports are planned to include more activities like administrator activity, violations, inactive accounts, etc.

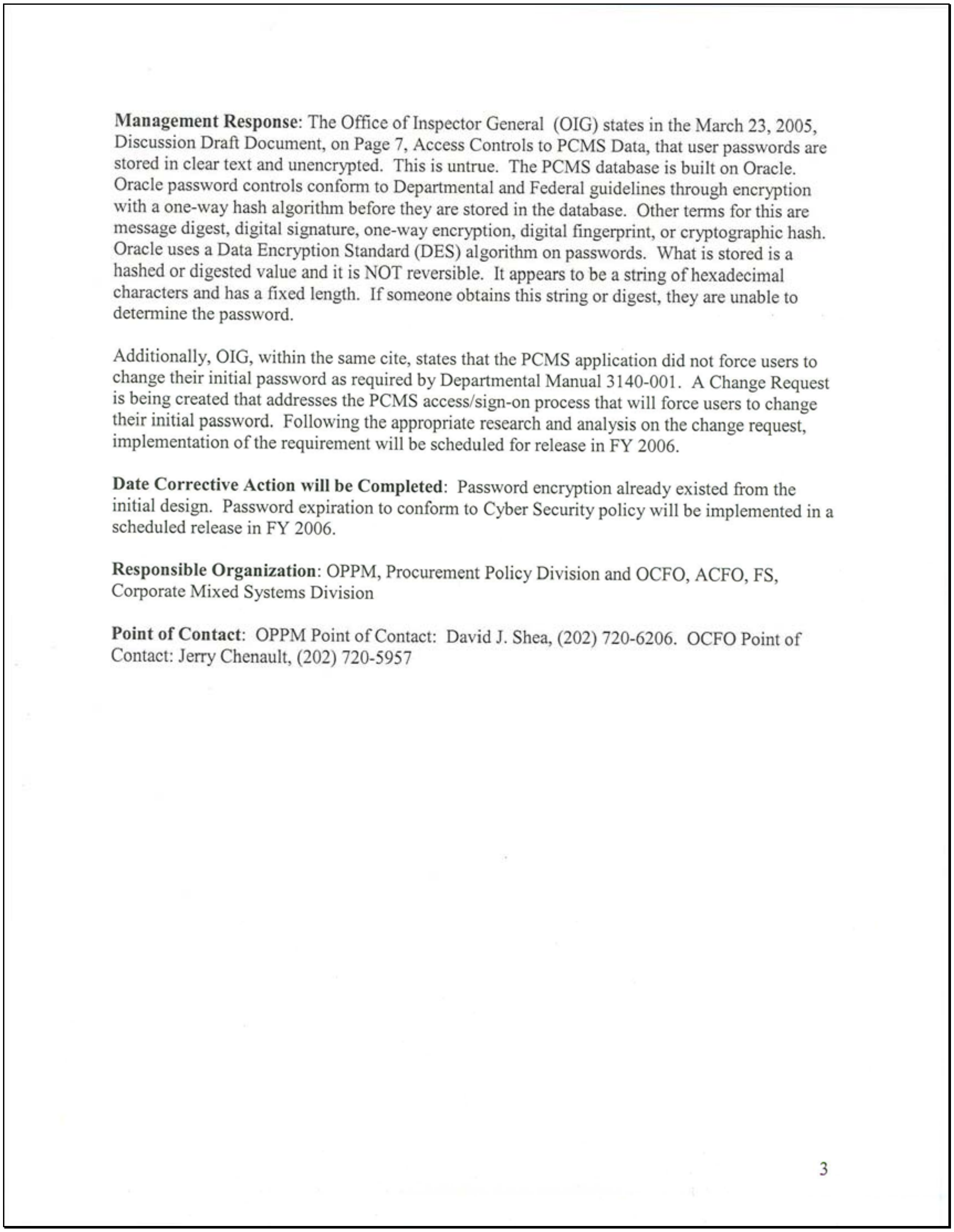
NFC role owners and ISSO are working together to implement role-based access and produce reports for management review of access and roles of their staff. Role based access and monitoring has been established for IRMD employees. ACFO-FS and ISSO will work together to implement role based security control monitoring for other OCFO employees by September 30, 2006.

Date Corrective Action will be Completed: Access privileges were reviewed, corrected and finalized in May 2005. ISSO's plan for role based security control monitoring and reporting on implementation for ACFO-FS is scheduled for September 30, 2006.

Responsible Organization: OPPM, Procurement Policy Division, OCFO, NFC, IRMD, and OCFO, ACFO, FS, Corporate Mixed Systems Division

Point of Contact: OPPM Point of Contact: David J. Shea, (202) 720-6206. OCFO Point of Contact for Data Base Administration: Gilbert Hawk, (504) 426-2000, OCFO Point of Contact for Role Based security access is Jerry Chenault, (202) 720-5957

Audit Recommendation No. 4: OCFO/NFC should modify the PCMS application to ensure that user password controls conform to departmental and Federal guidelines.



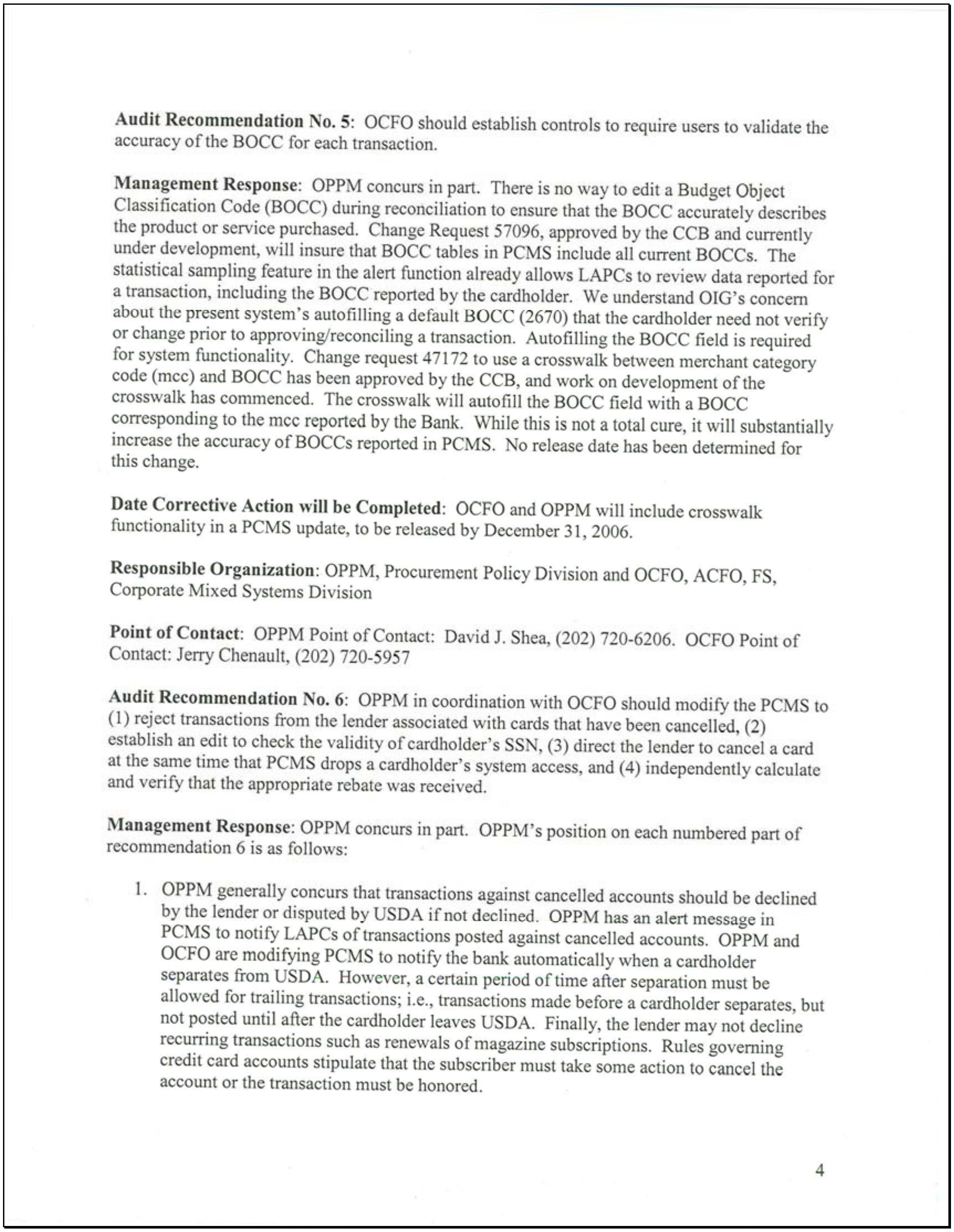
Management Response: The Office of Inspector General (OIG) states in the March 23, 2005, Discussion Draft Document, on Page 7, Access Controls to PCMS Data, that user passwords are stored in clear text and unencrypted. This is untrue. The PCMS database is built on Oracle. Oracle password controls conform to Departmental and Federal guidelines through encryption with a one-way hash algorithm before they are stored in the database. Other terms for this are message digest, digital signature, one-way encryption, digital fingerprint, or cryptographic hash. Oracle uses a Data Encryption Standard (DES) algorithm on passwords. What is stored is a hashed or digested value and it is NOT reversible. It appears to be a string of hexadecimal characters and has a fixed length. If someone obtains this string or digest, they are unable to determine the password.

Additionally, OIG, within the same cite, states that the PCMS application did not force users to change their initial password as required by Departmental Manual 3140-001. A Change Request is being created that addresses the PCMS access/sign-on process that will force users to change their initial password. Following the appropriate research and analysis on the change request, implementation of the requirement will be scheduled for release in FY 2006.

Date Corrective Action will be Completed: Password encryption already existed from the initial design. Password expiration to conform to Cyber Security policy will be implemented in a scheduled release in FY 2006.

Responsible Organization: OPPM, Procurement Policy Division and OCFO, ACFO, FS, Corporate Mixed Systems Division

Point of Contact: OPPM Point of Contact: David J. Shea, (202) 720-6206. OCFO Point of Contact: Jerry Chenault, (202) 720-5957



Audit Recommendation No. 5: OCFO should establish controls to require users to validate the accuracy of the BOCC for each transaction.

Management Response: OPPM concurs in part. There is no way to edit a Budget Object Classification Code (BOCC) during reconciliation to ensure that the BOCC accurately describes the product or service purchased. Change Request 57096, approved by the CCB and currently under development, will insure that BOCC tables in PCMS include all current BOCCs. The statistical sampling feature in the alert function already allows LAPCs to review data reported for a transaction, including the BOCC reported by the cardholder. We understand OIG's concern about the present system's autofilling a default BOCC (2670) that the cardholder need not verify or change prior to approving/reconciling a transaction. Autofilling the BOCC field is required for system functionality. Change request 47172 to use a crosswalk between merchant category code (mcc) and BOCC has been approved by the CCB, and work on development of the crosswalk has commenced. The crosswalk will autofill the BOCC field with a BOCC corresponding to the mcc reported by the Bank. While this is not a total cure, it will substantially increase the accuracy of BOCCs reported in PCMS. No release date has been determined for this change.

Date Corrective Action will be Completed: OCFO and OPPM will include crosswalk functionality in a PCMS update, to be released by December 31, 2006.

Responsible Organization: OPPM, Procurement Policy Division and OCFO, ACFO, FS, Corporate Mixed Systems Division

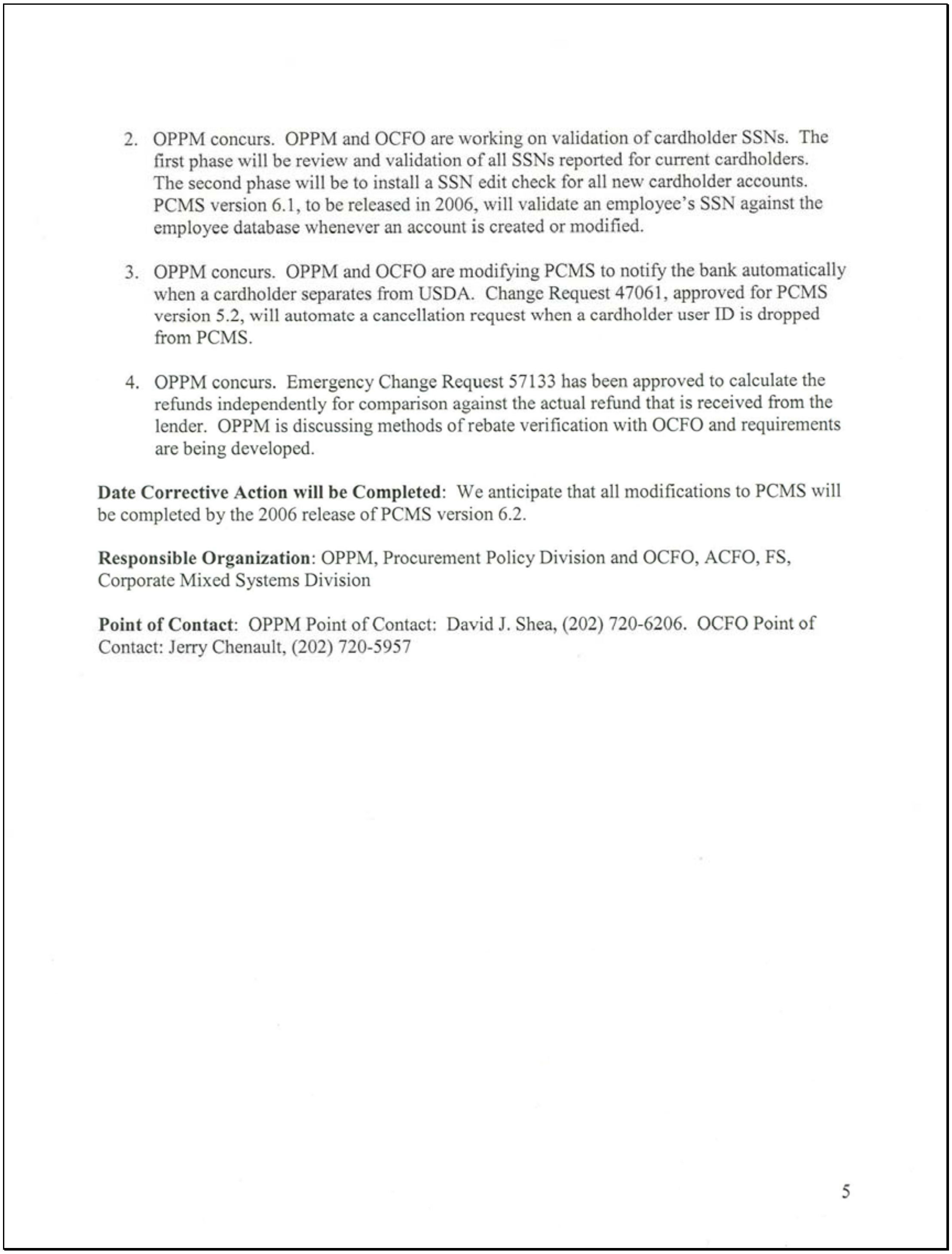
Point of Contact: OPPM Point of Contact: David J. Shea, (202) 720-6206. OCFO Point of Contact: Jerry Chenault, (202) 720-5957

Audit Recommendation No. 6: OPPM in coordination with OCFO should modify the PCMS to (1) reject transactions from the lender associated with cards that have been cancelled, (2) establish an edit to check the validity of cardholder's SSN, (3) direct the lender to cancel a card at the same time that PCMS drops a cardholder's system access, and (4) independently calculate and verify that the appropriate rebate was received.

Management Response: OPPM concurs in part. OPPM's position on each numbered part of recommendation 6 is as follows:

1. OPPM generally concurs that transactions against cancelled accounts should be declined by the lender or disputed by USDA if not declined. OPPM has an alert message in PCMS to notify LAPCs of transactions posted against cancelled accounts. OPPM and OCFO are modifying PCMS to notify the bank automatically when a cardholder separates from USDA. However, a certain period of time after separation must be allowed for trailing transactions; i.e., transactions made before a cardholder separates, but not posted until after the cardholder leaves USDA. Finally, the lender may not decline recurring transactions such as renewals of magazine subscriptions. Rules governing credit card accounts stipulate that the subscriber must take some action to cancel the account or the transaction must be honored.

Exhibit A – Agency Response to the Draft Report



2. OPPM concurs. OPPM and OCFO are working on validation of cardholder SSNs. The first phase will be review and validation of all SSNs reported for current cardholders. The second phase will be to install a SSN edit check for all new cardholder accounts. PCMS version 6.1, to be released in 2006, will validate an employee's SSN against the employee database whenever an account is created or modified.

3. OPPM concurs. OPPM and OCFO are modifying PCMS to notify the bank automatically when a cardholder separates from USDA. Change Request 47061, approved for PCMS version 5.2, will automate a cancellation request when a cardholder user ID is dropped from PCMS.

4. OPPM concurs. Emergency Change Request 57133 has been approved to calculate the refunds independently for comparison against the actual refund that is received from the lender. OPPM is discussing methods of rebate verification with OCFO and requirements are being developed.

Date Corrective Action will be Completed: We anticipate that all modifications to PCMS will be completed by the 2006 release of PCMS version 6.2.

Responsible Organization: OPPM, Procurement Policy Division and OCFO, ACFO, FS, Corporate Mixed Systems Division

Point of Contact: OPPM Point of Contact: David J. Shea, (202) 720-6206. OCFO Point of Contact: Jerry Chenault, (202) 720-5957