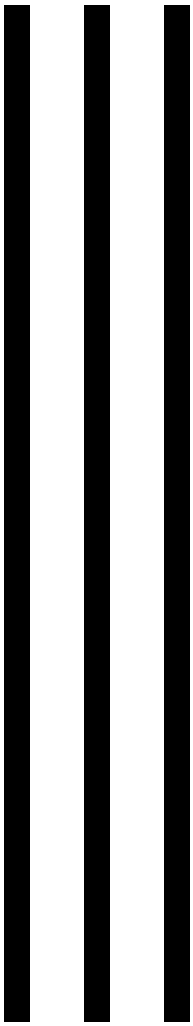

U.S. Department of Agriculture
Office of Inspector General
Financial and IT Operations
Audit Report

SECURITY OVER THE PURCHASE CARD MANAGEMENT SYSTEM

Report No.
50099-25-FM
JANUARY 2001

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington D.C. 20250

DATE: January 2, 2001

REPLY TO
ATTN OF: 50099-25-FM

SUBJECT: Security Over the Purchase Card Management System

TO: Sally Thompson
Chief Financial Officer
Office of the Chief Financial Officer

Paul W. Fiddick
Assistant Secretary
Department of Administration

This report presents the results of our audit of the Security Over the Purchase Card Management System. Your offices did not provide written comments to this report.

Since your offices did not provide a written response, we were unable to achieve management decision on any recommendations. In accordance with Departmental Regulation 1720-1, please furnish a reply within 60 days describing the corrective action taken or planned, including the timeframes on our recommendations. Please note that the regulation requires 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.

/s/

JAMES R. EBBITT
Assistant Inspector General
for Audit

EXECUTIVE SUMMARY

SECURITY OVER THE PURCHASE CARD MANAGEMENT SYSTEM
AUDIT REPORT NO. 50099-25-FM

PURPOSE

The audit was performed to ascertain whether Purchase Card Management System (PCMS) information technology resources were being appropriately secured by the Department.

RESULTS IN BRIEF

The OCFO/NFC has implemented an effective network security program. We found that physical security over the PCMS was good, and system software controls were in place and operating adequately. However, we did find several areas where PCMS was not in full compliance with provisions of the Office of Management and Budget's (OMB) Circular A-130, "Management of Federal Information Resources," or other regulatory requirements.

We noted the following problems.

- The PCMS had never been successfully tested at the Office of the Chief Financial Officer/National Finance Center's (OCFO/NFC) backup recovery operations center (ROC) because of administrative errors.

- Procedures that would permit PCMS to continue functioning if the operation of the general support systems[1] were interrupted due to a disaster had not been developed.

- System documentation was not available for the PCMS.

- Access security controls needed further strengthening for the PCMS. We found personnel with administrative access to the PCMS that were not authorized for this high level access.

[1] A "general support system" is 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.

- Assurances relating to the security of sensitive data transmitted between PCMS and the credit card vendor were not available.

KEY RECOMMENDATIONS

We recommended that the OCFO and/or the Assistant Secretary for Departmental Administration do the following.

- Prepare an application security plan for PCMS in accordance with OMB Circular A-130.
- Prepare detailed system design documentation for PCMS.
- Ensure that PCMS and related general support systems are periodically tested at the ROC and that local recovery operations are documented.
- Obtain assurances concerning the security of the dedicated line transmitting sensitive data in an unencrypted format.

AGENCY RESPONSE

The CFO and Assistant Secretary did not provide written comments to this audit.

TABLE OF CONTENTS

INTRODUCTION

BACKGROUND

The Purchase Card Management System (PCMS) is an online relational database management system of the U. S. Department of Agriculture. PCMS is used to manage Government purchase card (GPC) transactions.

Government employees (and authorized non-Government employees) use this system to track and control expenses. As of September 2000, for fiscal year (FY) 2000, PCMS processed about $450 million in credit card transactions and an additional $19 million in fleet card transactions. There are approximately 25,000 credit cards and approximately 43,000 fleet cards issued.

OBJECTIVES

Our audit objective was to identify and test the security policies and procedures placed into operation over PCMS and related support systems.

SCOPE

This audit was conducted in accordance with Government auditing standards. We performed this audit at the OCFO/NFC located in New Orleans, Louisiana. The audit scope was limited to reviewing selected security measures related to PCMS, not to validate payments or assess controls and/or security at user agencies. Our audit was performed during the period of November 1999 through September 2000.

METHODOLOGY

To accomplish our audit objectives, our examination consisted of the following.

- Review of policies and procedures governing the use of PCMS;
- Review of risk analyses and security plans related to PCMS;
- Review of database management control objectives and techniques;

- Perform vulnerability scans of various servers, routers, switches and fire walls; and

- Review of disaster recovery and contingency plans applicable to PCMS.

FINDINGS AND RECOMMENDATIONS

CHAPTER 1	OCFO/NFC's NETWORK SECURITY PROGRAM IS GENERALLY SOUND

FINDING NO. 1

Overall, the OCFO/NFC has implemented a sound network security system. We independently conducted vulnerability assessments of computer systems involved in the processing of PCMS transactions. We used a commercial off-the-shelf software product to perform these tests. This software performs over 800 tests for security vulnerabilities on systems that use Transmission Control Protocol/Internet Protocol. Our assessments identified no material problems for the equipment or software scanned.

We did find, however, that the OCFO/NFC uses a dedicated, high-speed data transmission line for transmitting financial, privacy and sensitive PCMS data between the credit card vendor and the OCFO/NFC. The data is transmitted over this line in clear text, even though other PCMS data is transmitted encrypted. While OCFO/NFC personnel advised us that the data is transmitted over a dedicated, communications line, it was not able to provide to us any vendor certifications or other assurances that the data transmitted over this line was, in fact, secure.

We discussed this matter with personnel from departmental administration who stated that they believed the data being transmitted over the dedicated line was encrypted using Oracle's Advanced Networking Option (ANO). However, we found that ANO was used to encrypt the data being transmitted by the users of the system, but that the data transmitted between the credit card vendor and OCFO/NFC was transmitted in clear text. Departmental administration personnel were also unable to provide us any certifications or other assurances that data being transmitted over the dedicated line was properly secured.

RECOMMENDATIONS TO THE OFFICE OF THE CHIEF FINANCIAL OFFICER AND ASSISTANT SECRETARY FOR ADMINISTRATION

RECOMMENDATION NO. 1	Obtain necessary certifications or assurances that the sensitive data transmitted between the vendor and the OCFO/NFC is properly secured.

CHAPTER 2 | OCFO/NFC NEEDS TO PERFORM REQUIRED A-130 REVIEW OF PCMS

The OCFO/NFC had not designated PCMS as a "major application" until March 2000; therefore, not all of the requirements of the Office of Management and Budget's (OMB) Circular A-130, "Management of Federal Information Systems," regarding controls for major applications had been applied to this critical system. As a result, an application that processed about $470 million in payments, during FY 2000, may not meet required security guidelines meant to ensure the reliability, confidentiality, and availability of critical PCMS data.

FINDING NO. 2

AN APPLICATION SECURITY PLAN AND SYSTEM DOCUMENTATION NEEDS TO BE COMPLETED

The Information Systems Policy and Control Staff (ISPCS) had not prepared an application security plan, as required by OMB Circular A-130[2]. Without an application security plan, the OCFO/NFC cannot assure that management, operations, personnel, and technical controls are functioning effectively and providing adequate levels of protection within PCMS. In addition, the Applications Systems Division (ASD) was not able to provide current system design documentation for PCMS.[3]

We found that a partial A-130 review of the PCMS had been conducted by the OCFO/NFC when the system was initiated. However, since that time, there have been significant changes concerning the platform that PCMS runs on, the network configuration, the overall size and complexity of PCMS, etc. Information Systems Security Office personnel said that PCMS is now considered to be a major application, and they will prepare an application security plan during the next fiscal year.

We contacted ASD to obtain current system documentation for the PCMS for our review. (System documentation should show system requirements, specifications, edits, etc.) However, we found that the existing documentation did not reflect the current system's design. We also noted that this problem was identified by a contractor in a report issued August 1996, the report stated: "There is a lack of the detailed documentation necessary to effectively specify, develop, and deploy a major computer system. The missing documents include: Detailed System Requirements, System Architecture, and Detailed System Design." This report recommended that OCFO/NFC develop detailed documentation to provide a baseline of the system specifications.

---

[2] OMB Circular A-130 states that the methods used to assess the nature and level of risk to the system should include a consideration of the major factors in risk management: the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards.

[3] This documentation would have detailed requirements and specifications for PCMS and is necessary to effectively specify, develop, and deploy a major computer system.

RECOMMENDATIONS TO THE OFFICE OF THE CHIEF FINANCIAL OFFICER AND ASSISTANT SECRETARY FOR ADMINISTRATION

RECOMMENDATION NO. 2

Prepare an application security plan for PCMS in accordance with OMB Circular A-130 and the guidance provided by National Institute of Standards and Technology.

RECOMMENDATION NO. 3

Develop appropriate control objectives and techniques for the PCMS based upon this risk assessment.

RECOMMENDATION NO. 4

Complete necessary documentation for PCMS to include detailed system requirements, system architecture, and a detailed system design.

FINDING NO. 3

CONTINGENCY PLANS NEED TO BE COMPLETED

The Department had not developed procedures that would permit PCMS to continue functioning if service continuity was interrupted. ISPCS personnel stated that the Information Technology (IT) systems used to process PCMS have changed frequently and until the system stabilized, they did not develop a plan for disaster recovery operations. Without adequate service continuity planning, the system would not be available for processing during service interruptions. We believe this is unacceptable for a system that processed about $470 million in credit card transactions during FY 2000.

The OCFO/NFC developed a Disaster Recovery Plan, dated March 4, 1998, which provides for the restoration of OCFO/NFC's critical business operations within 24 to 48 hours of experiencing a significant disruption to the IT capabilities. It has also developed the Open Systems Disaster Recovery Procedures, dated November 4, 1999, which provides for restoring the various support systems of OCFO/NFC (e.g., proxy server, firewall servers, voice response system, etc.). However, neither of these plans include restoration policies and procedures for the PCMS at the ROC.

Although PCMS is a Departmentwide application, that processes transactions for over 68,000 of credit card and fleet card users, assessments have not been completed within the Department to identify the range of potential disruptions that would need to be mitigated to avoid service interruptions. (Potential disruptions range from minor interruptions such as, temporary power failures; to major disasters such as fires, natural disasters, or denial of service attacks.)

RECOMMENDATIONS TO THE OFFICE OF THE CHIEF FINANCIAL OFFICER AND ASSISTANT SECRETARY FOR ADMINISTRATION

RECOMMENDATION NO. 5

Assess and document the risks and threats, both internal and external, associated with the processing of PCMS. Include the extent to which loss of services to PCMS can be tolerated, and institute appropriate controls to mitigate the impact of service interruptions.

RECOMMENDATIONS TO THE OFFICE OF THE CHIEF FINANCIAL OFFICER

RECOMMENDATION NO. 6

Ensure that PCMS and the related general support systems are periodically tested at remote sites. Document any necessary local recovery operations.

CHAPTER 3 | OCFO/NFC NEEDS TO STRENGTHEN ACCESS SECURITY OVER PCMS

Access controls over PCMS need to be further strengthened. OCFO/NFC personnel did not fully follow established policies and procedures relating to controlling access to sensitive systems. As a result, security over this system was reduced.

FINDING NO. 4

We found that there were 34 user identifications (ID's) that had Data Base Administrator (DBA) access to the PCMS database. Our review found the following problems: (1) 10 of these ID's belonged to 5 users and allowed duplicate access privileges; (2) one user, who had DBA authorities, was no longer performing DBA functions; (3) one user ID, belonging to an individual who had DBA authorities, no longer worked at the OCFO/NFC; (4) one user was granted DBA authorities in order to change passwords although DBA authorities are not needed for this purpose; and (5) two of six Oracle "default" passwords had not been changed from the default passwords -- a significant vulnerability. OCFO/NFC personnel changed the default passwords when we identified this problem to them, and they revoked the DBA access from the person who no longer worked at OCFO/NFC.

We also found that the forms approving access to the PCMS could not be located for several users. We requested the Form OCFO/NFC-1106, Security Access Request, for each of the 34 users that had been granted DBA authorities. We were able to obtain only 17 of the 34 required forms. We also noted that the forms did not always contain the required information such as the "Resource Owner" signature and approval.

RECOMMENDATIONS TO THE OFFICE OF THE CHIEF FINANCIAL OFFICER

RECOMMENDATION NO. 7

Review the needs of each of the user ID's granted DBA authorities and ensure each user requires that level of access.

RECOMMENDATION NO. 8

Ensure that there is a properly prepared and approved Security Access Request form for each user granted access.

ABBREVIATIONS

ASD	Applications Systems Division
ANO	Advanced Networking Option
DBA	Database Administrator
FY	Fiscal Year
GPC	Government Purchase Card
ID	Identification
ISPCS	Information Systems Policy and Control Staff
IT	Information Technology
OCFO/NFC	Office of the Chief Financial Officer/National Finance Center
OIG	Office of Inspector General
OMB	Office of Management and Budget
PCMS	Purchase Card Management System
ROC	Recovery Operations Center