NPS-GSBPP-11-007

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

IDENTIFYING PROCUREMENT FRAUD IN DEFENSE AGENCIES: AN ANALYSIS OF THE GOVERNMENT PURCHASE CARD PROGRAM

by

Juanita M. Rendon, Lecturer

April 2011

Graduate School of Business & Public Policy

Naval Postgraduate School

Prepared for: Naval Postgraduate School, Monterey, California 93943

THIS PAGE INTENTIONALLY LEFT BLANK

NAVAL POSTGRADUATE SCHOOL
Monterey, California 93943-5000

Daniel T. Oliver
President

Leonard A. Ferrari
Executive Vice President and
Provost

The report entitled *"Identifying Procurement Fraud in Defense Agencies: An Analysis of the Government Purchase Card Program"* was prepared for and funded by the Acquisition Program, Graduate School of Business & Public Policy, Naval Postgraduate School.

This report was prepared by:

Juanita M. Rendon
Lecturer
Graduate School of Business & Public Policy

Reviewed by:

William R. Gates, Ph.D.
Dean, Graduate School of Business
& Public Policy

Released by:

Douglas Fouts, Ph.D.
Interim Vice President and
Dean of Research

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form approved
OMB No 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	18 April 2011	**Technical Report**

4. TITLE AND SUBTITLE
Identifying Procurement Fraud in Defense Agencies: An Analysis of the Government Purchase Card Program

5. FUNDING

6. AUTHOR (S)
Juanita M. Rendon

7. PERFORMING ORGANIZATION NAME (S) AND ADDRESS (ES)
NAVAL POSTGRADUATE SCHOOL
GRADUATE SCHOOL OF BUSINESS AND PUBLIC POLICY
555 DYER ROAD
MONTEREY, CA 93943-5103

8. PERFORMING ORGANIZATION REPORT NUMBER
NPS-GSBPP-11-007

9. SPONSORING/MONITORING AGENCY NAME (S) AND ADDRESS (ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words.)
This research explores the Department of Defense (DoD) Government Purchase Card Program. The specific purpose of this research is to identify fraud indicators within the DoD Government Purchase Card Programs. This research identifies fraud indicators within the DoD Government Purchase Card Programs and provides recommendations for improving the management of Government Purchase Card Programs within the DoD. First, a brief background of the DoD Government Purchase Card Program is provided. Second, based on GAO reports and OIG audits, incidents of procurement card fraud are discussed. Third, fraud indicators in Government Purchase Card Programs are identified. Fourth, Government Purchase Card Program Internal Control Issues are addressed. Finally, the research concludes with a summary and areas for further research.

14. SUBJECT TERMS
Department of Defense, government purchase card programs, fraud indicators, internal control

15. NUMBER OF PAGES 63

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT: UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE: UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT: UNCLASSIFIED	20. LIMITATION OF ABSTRACT: UU

NSN 7540-01-280-5800
Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Abstract

This research explores the Department of Defense (DoD) Government Purchase Card Program.. This research identifies fraud indicators within the DoD Government Purchase Card Programs and provides recommendations for improving the management of Government Purchase Card Programs within the DoD. First, a brief background of the DoD Government Purchase Card Program is provided. Second, based on GAO reports and OIG audits, incidents of procurement card fraud are discussed. Third, fraud indicators in Government Purchase Card Programs are identified. Fourth, Government Purchase Card Program Internal Control Issues are addressed. Finally, the research concludes with a summary and areas for further research.

Keywords: Department of Defense, government purchase card programs, fraud indicators, internal control

THIS PAGE INTENTIONALLY LEFT BLANK

Acknowledgments

Sincere thanks go to RADM James B. Greene, USN (Ret.), the NPS Acquisition Chair, for securing funding of this research and to Dr. Keith F. Snider, Associate Professor of Public Administration and Management, for his support. In addition, special thanks to Karey Shaffer and Tera Yoder of the NPS Acquisition Research Program office for their dedication, support, and guidance. This research report would not have been possible without their assistance. Special thanks also to Dr. Rene G. Rendon, Associate Professor of Acquisition Management, for his constant support and encouragement, for which I am eternally grateful. I thank the Lord for His amazing grace, mercy, and faithfulness and for all of His abundant blessings in my life. May He be glorified in all things.

THIS PAGE INTENTIONALLY LEFT BLANK

About the Authors

Juanita M. Rendon teaches auditing, finance, and accounting courses at the Naval Postgraduate School. She is a CPA and former IRS Revenue Agent. She is a member of the AICPA and the Association of Certified Fraud Examiners.

She has published articles in the *Journal of Contract Management* and book chapters in *Cost Estimating and Contract Pricing* (2008) and in *Contract Administration* (2009) by Gregory A. Garrett. She has presented at the NCMA World Congress conferences, as well as at NCMA's National Education Seminars, and was the recipient of the 2008 NCMA Award for Excellence in Contract Management Research and Writing.

Juanita M. Rendon
Graduate School of Business and Public Policy
Naval Postgraduate School
Monterey, CA 93943-5000
Tel: 831-656-2444
Fax: (831) 656-3407
E-mail: jmrendon@nps.edu

THIS PAGE INTENTIONALLY LEFT BLANK

Table of Contents

THIS PAGE INTENTIONALLY LEFT BLANK

Executive Summary

The general public demands better stewardship, efficient management of funds, and greater accountability for resources by government organizations (Mills, Normand, & Palmer, 2008). While the increased use of purchase cards has been determined to be beneficial in terms of cost reductions and decreased red tape processing procedures, there has also been a marked increase in misuse and fraudulent activity in purchase card programs throughout government agencies, including the Department of Defense (DoD) (Government Accountability Office [GAO], 2008, 2001).

In light of all the recent federal procurement scandals, the emergence of additional guidance for government purchase card programs (GPCP) has been steadily increasing. The more approving officials and cardholders are aware of perceived weaknesses in internal controls, the more likely they will be to take appropriate steps to reduce the potential for fraudulent activities. Potential indicators of fraudulent activity are clues or red flags that warrant a closer investigation into a certain area or activity. Intent is the key determining factor as to whether a particular situation is deemed fraud or mere negligence. The DoD Inspector General's website, as well as other agency sites, provides fraud guidance for their auditors, citing numerous, but not all-inclusive, possible purchase card fraud indicators.

DoD Inspector General audits of GPCPs agency-wide have resulted in the identification of various purchase card fraud indicators, such as cardholders making unauthorized purchases over the weekend or off-duty hours, cardholders and/or approving officials not adhering to policies and management controls, cardholders approving their own purchase authorizations instead of following required authorization mandates, and cardholders not following policies regarding separation of duties (GAO, 2003; DoD Inspector General [DoDIG], 2010, 2007).

Federal government officials, such as GPCP approving officials and cardholders, hold a public trust and are expected to meet the highest ethical

standards, especially when working with millions of taxpayer dollars on behalf of the American people. Because fraud is a serious problem throughout the nation and in the public procurement arena, it is crucial that procurement officials receive the appropriate training and learn the skills necessary to deter and detect fraud within agency-wide GPCPs. Unfortunately, many government executives have failed to implement and follow the existing internal control policies that are in place to help deter and detect fraudulent activities (GAO, 2008).

This research explores the DoD GPCP. This research identifies fraud indicators within the DoD GPCPs and provides recommendations for improving the management of the GPCPs within the DoD. First, a brief background of the DoD GPCP is provided. Second, based on GAO reports and Office of Inspector General (OIG) audits, incidents of procurement card fraud are discussed. Third, fraud indicators in the GPCPs are identified. Fourth, the GPCP internal control issues are addressed. Finally, the research concludes with a summary and areas for further research.

I. Introduction

The purpose of this research paper is to identify procurement fraud indicators in Defense agencies, specifically in the area of GPCPs. The areas covered in this research paper include a brief background of the Department of Defense (DoD) Government Purchase Card Program, a discussion of incidents of procurement card fraud, and the identification of fraud indicators in the GPCPs. In addition, the GPCP internal control issues are also addressed. A summary and conclusion will be provided, and areas for further research will be identified.

As of 2006, the United States GPCP was approximately eight times larger than the next largest purchase card program in the commercial card world (Fischer, 2006). With billions of taxpayer dollars being spent on goods and services by the federal government on behalf of the American people, the general public demands better stewardship, efficient management of funds, and greater accountability for resources by government organizations (Mills, Normand, & Palmer, 2008). Over the years, the government purchase card program has become an increasingly valuable and vital tool in government agencies in efforts to streamline their procurement process and meet their missions, especially in the DoD. The following section will provide a brief background of the DoD GPCP.

A. Background of Department of Defense Government Purchase Card Program

The subject of government purchase cards dates back to 1982 when President Ronald Reagan issued an executive order directing executive government agencies to decrease administrative procurement costs (Government Accountability Office [GAO], 1996). The overall goals of the GPCP are to save taxpayer money by reducing the administrative costs associated with the purchase of commercially available goods and services, and by reducing the procurement red tape and lead time involved in the normal procurement process (General Services Administration [GSA], 2011a).

Federal agencies acquire purchase cards from banks that have been awarded contracts under the GSA SmartPay program. U.S. Bank services the Army, Air Force, and Defense agencies, and Citibank services the Navy and Marine Corps (DoD, 2002).

The Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics (OUSD[AT&L]) oversees the agency-wide government purchase card program (GPCP). The Purchase Card Program Management Office (PCPMO) is responsible for policy formulation, procedural guidance, and operational oversight of the GPCP administered by DoD components, and it reports to the Director of Defense Procurement and Acquisition Policy in the OUSD(AT&L).

The Defense Procurement and Acquisition Policy (DPAP) office, headed by Mr. Shay Assad, is responsible for all acquisition and procurement policy matters in the DoD and serves as the main advisor to the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD[AT&L]) and the Defense Acquisition Board on acquisition/procurement strategies for all major weapon systems programs, major automated information systems programs, and services acquisitions (DPAP, 2011). Federal Acquisition Regulation (FAR), Part 13 (2011), and the Defense Federal Acquisition Regulation Supplement (DFARS), Part 213 (1999), govern the use of purchase cards (DoD, 2002).

The SmartPay Program, known as the largest government charge card program in the world, provides 350 federal agencies, organizations, and tribal governments' commercial charge card-based procurement and payment assistance to make efficient and convenient procurement transactions. According to the GSA, which administers the program under a master contract, the SmartPay Program has saved federal agencies an estimated $1.8 billion in annual administrative processing costs, as compared to previous, paper-based procurement card processes. The Office of Charge Card Management (OCCM) within GSA manages the GSA SmartPay Program (GSA, 2011d; Office of Management and Budget [OMB], 2009).

The use of government purchase cards has skyrocketed since the purchase cards first became available in 1986. Struebing (1996) found that during the first year that the government purchase cards were made available agency-wide, there were approximately 271,000 purchases made, worth approximately 64 million taxpayer dollars. By the end of FY1995, cardholders used the purchase card to purchase more than 1.6 billion taxpayer dollars worth of goods and services (Struebing, 1996). Most government officials agree that the FAR needs to address the use of government purchase cards more thoroughly and provide ways in which government agencies can share best practices in the area of purchase card programs (GAO, 1996).

As shown in Figure 1, during FY2009, the agency-wide government purchase card program, which includes purchase, travel, and fleet cards, totaled 3.1 million cardholders, 93.2 million transactions, and $29.8 billion in spending; and during FY2010, the GPCP program totaled 3.1 million cardholders, 98.9 million in transactions, and $30.2 billion in spending (GSA, 2011). This is quite an accomplishment, given that the government purchase card program initially experienced a slow start in the 1980s. Even though the program was widely recognized as a good opportunity to streamline payments and reduce cost, at first, it was not fully supported by all federal agencies (Fischer, 2006). For 2010, the Department of Defense was the top agency by program spend, with more than $13,257,132,377, or 44% of total spend (GSA, 2011c).

Fischer (2006) notes that the Federal Acquisition Streamlining Act of 1994, which authorized an increase to the mirco-purchase dollar value up to $2,500 (currently $3,000) for any single purchase, along with the mandated reinventing government initiative, helped catapult the GPCP, resulting in significant growth of the agency-wide program. Empowered agency administrators suddenly embraced the government purchase card as a tool to help them reduce cost and improve efficiencies within their agencies.

Even though the DoD Charge Card Task Force (DoD, 2002) noted that the cost savings is estimated to be approximately $20 per transaction, according to the GSA, federal government agencies save approximately $53.77 in administrative costs for each card purchase and payment, as compared to the normal procurement process involving a check payment (Fischer, 2006). Palmer, Gupta, and Dawson (2010) note that the federal government estimates cost savings from using the government purchase card to be in the range of $54 to $92 per transaction, with the best estimate being $69 per transaction, when compared to the cost of the paper processing of a purchase order, requisition, and payment. While the amount of savings per transaction may vary, it is still a well-documented fact that there is a cost savings benefit from using purchase cards (Fischer, 2006; Palmer, Gupta, & Dawson, 2010; DoD, 2002).

Use of the purchase card has allowed DoD federal agencies to replace the time-consuming paper-based purchase order process for micro-purchases, which results in lower procurement lead time, transaction cost, and procurement office workload. As of FY2001, DoD agencies use purchase cards for over 95% of qualified transactions (DoD, 2002). According to the GSA, only 2% of the total federal government spending are purchases under $2,500, but constitute over 85% of the total procurement transaction volume. The GSA has determined that the use of purchase cards has decreased the time that is required to properly process paper transactions by two to six weeks (Palmer, Gupta, & Dawson, 2010). In addition, the average government purchase card transaction amount has steadily increased from $436 in 1997, to $779 in 2008 (Palmer, Gupta, & Dawson, 2010).

The GSA SmartPay program office provides government charge cards to U.S. government federal agencies through negotiated master contracts with charge card providers. Currently, Citibank, JPMorgan Chase, and U.S. Bank provide the following types of charge cards to federal agencies to support their mission needs (GSA, 2011a):

- **Purchase Cards:** For purchases of general supplies and services;

- **Travel Cards:** For payment of travel expenses related to official government travel (airline, hotel, meals, incidentals);
- **Fleet Cards:** For payment of fuel and supplies for government vehicles; and
- **Integrated Cards:** For procurements of two or more business lines (card types) whose processes are integrated into one card.

While there are several types of government charge cards, the focus of this research was on the purchase cards. Figure 2, GSA SmartPay Program—Purchase Card (FY1999 to FY2008), shows a downward trend for the number of cardholders, yet an upward trend in purchase card transactions and purchase card spending. Even though in 2009, the number of cardholders, transactions, and spending slightly decreased, currently, the number of cardholders remains steady, while the number of transactions and spending continues to increase (GSA, 2011b).

Total	FY 2008	FY 2009	FY 2010
Spend	$30.6 B	$29.8 B	$30.2 B
Transactions	100.3 M	93.2 M	98.9 M
Cardholders	3.2 M	3.1 M	3.1 M

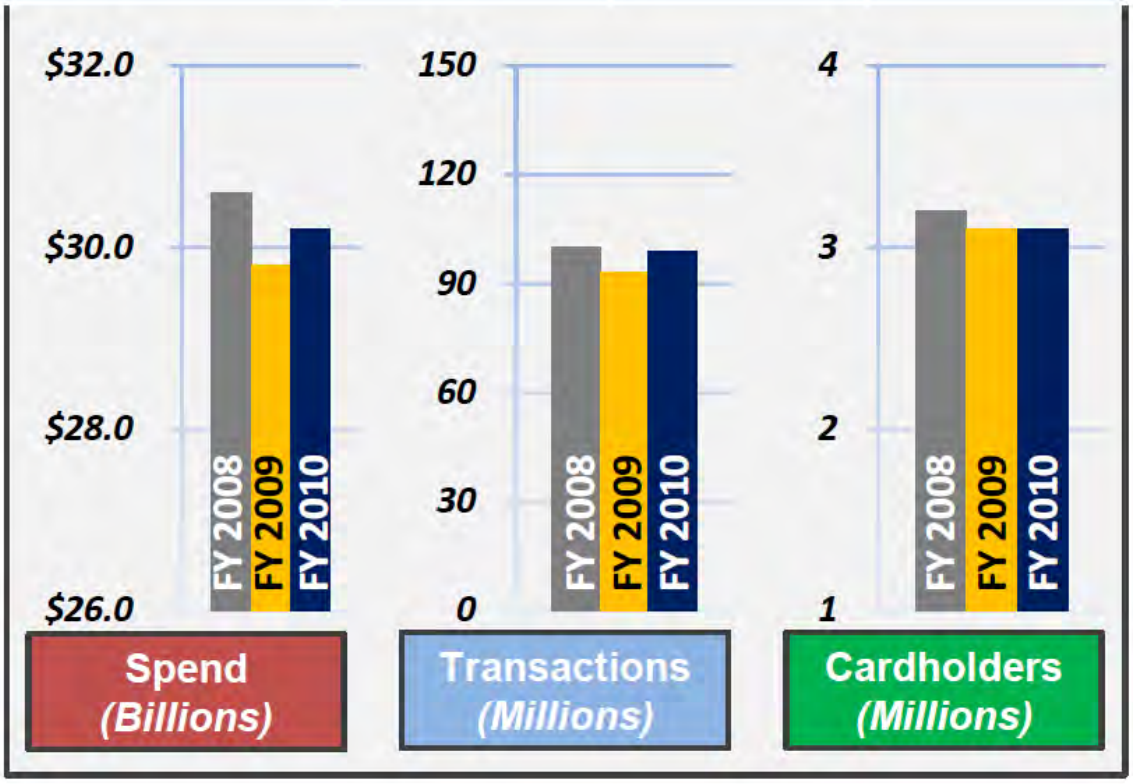

Figure 1. Fiscal Year 2010 GSA SmartPay Program
(GSA, 2011b)

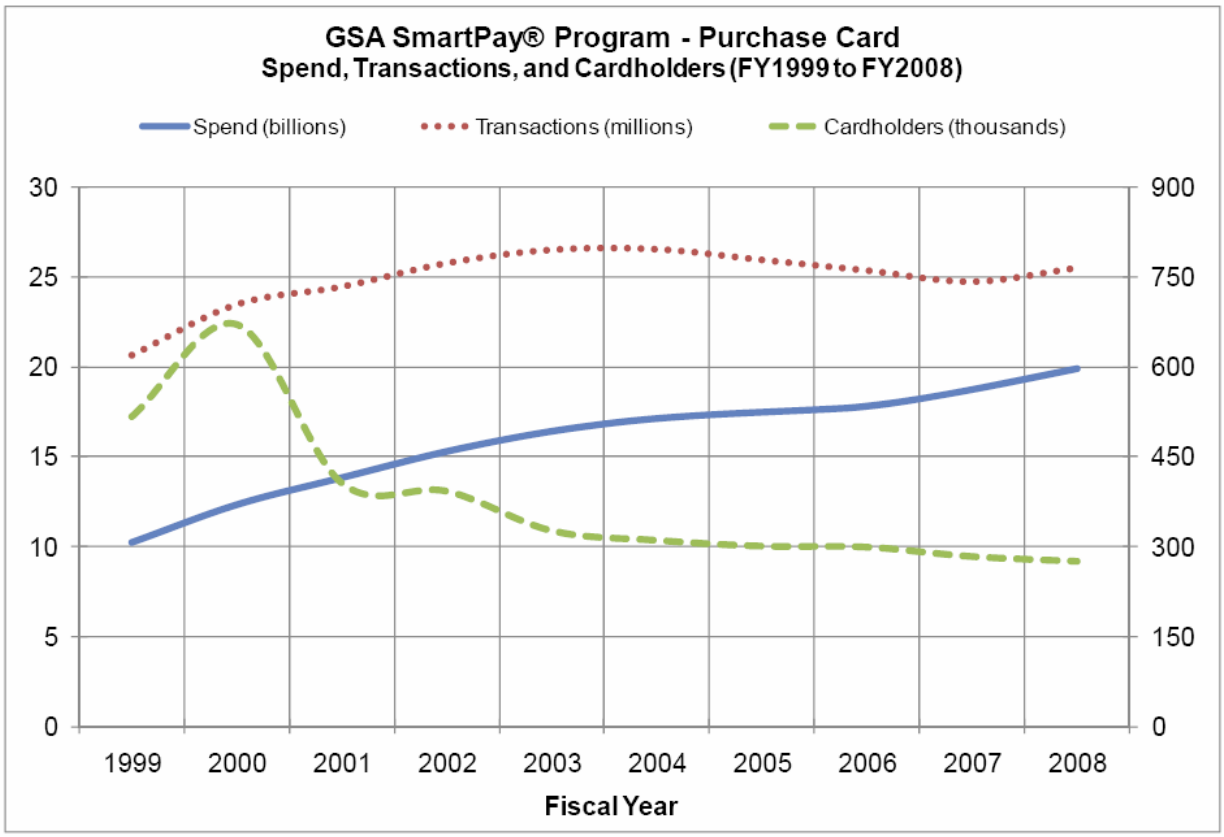

Figure 2. GSA SmartPay Program—Purchase Card (FY1999 to FY2008)
(GSA, 2011c)

On January 15, 2009, the OMB issued OMB Circular A-123, Appendix B Revised, in efforts to consolidate current government-wide charge card program requirements and guidance issued by the OMB, GSA, Department of the Treasury (Treasury), and other federal agencies (OMB, 2009).

According to the *Treasury Financial Manual for Guidance of Departments and Agencies* (TFM 4-4500), the government-wide commercial purchase card may be used to do the following (FMR, 2010):

1. Make micro-purchases (currently $3,000);
2. Place a task or delivery order (if authorized in the basic contract, basic ordering agreement, or blanket purchase agreement); or
3. Make payments when the contractor agrees to accept payment by the purchase card.

Per the Defense Acquisition University (DAU) training materials for the online GPCP course, the DFARS (1999) 213.270 states that, except under certain limited circumstances, the government purchase card is the mandatory method of purchase and/or payment at or below the micro-purchase threshold, currently $3,000 (DAU, 2010). There are several key players in a government purchase card program, which include the agency/organization program coordinator (APC), the supervisor, the approving official (AO), the certifying official (CO), and the cardholder. For the DoD, the Approving Official acts as the Certifying Official; and for the U.S. Air Force, the Financial Service Officer (FSO) serves as the Certifying Officer (DAU, 2010).

All of these players have important roles within the GPCP and are held to a high standard of integrity (DAU, 2010). They each hold a public trust and are expected to meet the highest ethical standards. One of these key players is the cardholder who is responsible for the following (DAU, 2010):

- Completing the proper GPCP training,
- Receiving the proper authorization in accordance with agency procedures,
- Making sure the card is used "For Official Use Only,"
- Providing accurate information and data to the GPCP Certifying Official,
- Seeking the advice from the activity fiscal attorney when questioning use of funds for specific purchases, and
- Reporting any abuse, misuse, or fraud.

Another key player is the AO (or billing official) who is usually the cardholder's direct supervisor or someone who can influence the cardholder's performance appraisal and recommend any warranted disciplinary action when necessary. Some of the AO's roles and responsibilities include the following (DAU, 2010):

- Making sure that cardholder transactions meet the legal requirements for authorized purchase card transactions,

- Verifying adequate supporting documentation for any purchase card transactions,
- Confirming the completeness and accuracy of the facts presented in the cardholder's documentation,
- Ensuring that cardholders follow all required policies and procedures regarding government purchase card acquisitions,
- Retaining certified billing statements and supporting documents for the prescribed length of time according to Federal Acquisition Regulations, and
- Reporting any abuse, misuse, or fraud.

Furthermore, as stated in the DAU (2010) online training course, federal agencies must minimize conflict of interest issues when appointing Approving Officials by adequately and appropriately implementing separation of duties, which helps in the determent of fraud or embezzlement.

Although credit worthiness evaluations are required for travel cardholders, the credit worthiness evaluations for new purchase card applicants are no longer legislatively mandated, due to the passage of the 2006 Consolidated Appropriations Act. However, agency officials and charge card managers are allowed to continue requiring these evaluations at their discretion, as they consider the risks involved with charge card issuance (OMB, 2009). It is the author's opinion that the credit worthiness evaluations should be required for purchase cardholders as they are for travel cardholders. It is imperative that all cardholders are evaluated for credit worthiness since they are being put in a position to spend taxpayer dollars, especially during challenging economic times. It does not make sense to allow a government employee who has a bad credit rating to use a government credit card.

In addition, non-procurement cardholders are not subject to the same restrictions as contracting officers, nor do they have the extensive training, education, or experience that contracting officers have. Non-procurement cardholders generally have the benefit of free discretion when selecting vendors, products, and services, which, if left unchecked, could lead to abusive or even

fraudulent behavior when using the government purchase card. The following section will discuss incidents of government procurement card fraud as identified in some GAO and OIG government purchase card program audit results.

B. Incidents of Government Procurement Card Fraud

The DoD GPCP is subject to periodic audits in accordance with Title 10 *United States Code* (U.S.C.), section 2784(b)(8), by the DoD Inspector General and the military Services' audit agencies (DoD, 2010c).

Over the years, the escalating federal government procurement fraud scandals have created a need to seriously revisit the reality of the epidemic of procurement fraudulent activities across federal agencies. In 2002, the GAO found significant internal control weaknesses in government agency purchase card programs that allowed cardholders to make fraudulent purchases (GAO, 2002a; GAO 2002b). Also in 2002, the Defense Criminal Investigative Service (DCIS) opened investigations which involved individuals allegedly involved in credit card fraud. Additionally, the DCIS completed cases which have resulted in jail terms and probation, as well as restitution (Kozaryn, 2002).

According to a GAO (2008) report, even though the purchase card is an effective tool that helps agencies reduce transaction costs for small purchases and provides flexibility in making acquisitions, internal controls breakdowns and weaknesses over the use of purchase cards leave the government highly vulnerable to fraud, waste, and abuse. Table 1 illustrates examples of how the government purchase card has been flagrantly misused and abused. Some issues with the inappropriate and fraudulent card use include problems with transaction authorization, receipt and acceptance of goods purchased, and accountability of property acquired with the government purchase card. The GAO made recommendations to improve internal control and oversight of the GPCP in efforts to reduce instances of fraudulent, improper, and abusive purchases.

The GAO defines fraudulent, improper, and abusive transactions as follows:

> Fraudulent purchases or transactions include those made by cardholders that were unauthorized and intended for personal use, purchases made using purchase cards or account numbers that had been stolen or compromised, and purchases appropriately charged to the purchase card but that involve potentially fraudulent activity that went undetected because of the lack of integration among processes related to the purchase, such as travel claims or missing property.
>
> Improper transactions are those purchases that although intended for government use, are not permitted by law, regulation, or government/agency policy.
>
> Abusive purchase card transactions involve transactions that are deficient and improper when compared with behavior that a prudent person would consider reasonable and necessary, for example, purchases that were made at excessive cost (wasteful) or were not needed by the government, or both (GAO, 2008, p. 20).

In 2008, the GAO identified fraudulent, improper, and abusive activity in government-wide purchase card programs and made thirteen recommendations to the General Services Administration (GSA) and the Office of Management and Budget (OMB) in efforts to minimize fraudulent, improper, and abusive card activities and to improve oversight of purchase cards (GAO, 2008). While the OMB, which is taking a proactive approach to purchase card management, agreed with the recommendations, the GSA only partially agreed. Even though the GSA manages the government purchase card program, the GSA did not concur that it had the authority to assist government agencies with improving their internal controls. The OMB may be able to assist the GSA in overcoming the lack of authority perception (GAO, 2008).

Weaknesses and breakdowns in internal controls in government purchase card programs government-wide caused numerous fraudulent, improper, and abusive activities. Table 1 reveals some of the fraudulent, improper, and abusive activities that the GAO found, including a case in which a cardholder embezzled over $642,000 from the Department of Agriculture's Forest Service firefighting fund. The fraudulent activities, which took place over a period of six years, were not detected until 2006, when a whistleblower reported the cardholder to the agency's Office of Inspector General. This particular cardholder, who used the embezzled

funds to pay for personal expenses, such as gambling and mortgage payments, was ordered to pay full restitution and sentenced to 21 months in prison (GAO, 2008).

Table 1. Fraudulent, Improper, and Abusive Purchases by Cardholders
(GAO, 2008)

Fraudulent, Improper, and Abusive Purchases by Cardholders			
Type of purchase	**Agency**	**Amount**	**Activity**
Fraudulent	Department of Agriculture	$642,000	Cardholder used convenience checks to embezzle public funds for over 6 years. The $642,000 was used for personal expenditures, such as gambling, car and mortgage payments, and other retail purchases.
Improper	Department of Energy	112,300	Cardholder improperly used convenience checks—and consequently had to pay thousands in fees—for relocation services. Agency policy generally prohibits convenience checks above $3,000.
Abusive	Department of Defense	77,700	Four cardholders purchased expensive suits and accessories from Brooks Brothers and other high-end clothing stores to outfit several servicemembers.

Source: GAO analysis of bank data and supporting documentation.

Tables 2–5 illustrate incidents in which fraud or indications of fraud were found after investigations of government purchase card programs agency-wide by the GAO (2008). Some examples of fraud include purchases of online dating services by Army officials and U.S. Postal Service officials, as well as numerous instances of personal use purchases. In addition, the GAO found that agencies were not able to account for $2.7 million of pilferable items such as laptop computers, iPods, and digital cameras (GAO, 2008).

Once fraud is suspected, notification should be made to the Management Control Administrator, and the approving official (or billing official) or the Agency Program Coordinator (APC) should contact their respective law enforcement agency, such as the DoD Criminal Investigation Service (DCIS), Federal Bureau of Investigations (FBI), Naval Criminal Investigative Services (NCIS), United States Army Criminal Investigation Command (USACIDC), or Air Force Office of Special Investigations (AFOSI), or contact the DoD fraud hotline.

Table 2. Fraudulent and Potentially Fraudulent Activity

(GAO, 2008, p. 21)

Case	Description of activity	Vendor	Agency	Amount	Additional facts
1	Convenience checks Fraudulent use	None	Forest Service, USDA	$642,000	• During a 6-year period, the cardholder fraudulently wrote approximately 180 checks to an individual with whom the cardholder lived and shared a bank account. All transactions were undetected by the agency. • USDA's Office of Inspector General received a tip from a whistleblower that started the investigation leading to the cardholder's indictment in November 2006. • In June 2007, the cardholder pled guilty to embezzlement and tax fraud charges. • The cardholder was sentenced in November 2007 to 21 months imprisonment followed by 36 months of supervised release and was required to pay over $642,000 in restitution.
2	Lost computer equipment Potentially fraudulent transaction	CompUSA	Navy	2,200	• Cardholder purchased 19 pilferable items, including 2 LCD monitors, 5 iPods, a laser jet printer, a PDA, and other computer accessories, 18 of which are now lost and presumed stolen. • The cardholder is no longer with the Navy command. • The Navy could not provide documentation showing that the purchase was properly approved, that the requester received the items, or that the Navy had possession of 18 of the 19 items.

Table 3. Fraudulent and Potentially Fraudulent Activity

(GAO, 2008, p. 22)

Case	Description of activity	Vendor	Agency	Amount	Additional facts
3	Cosmetics Compromised account	Tina Nails, MAC	National Science Foundation	1,800	• The government purchase card was used to transact over $1,800 in fraudulent purchases at a nail salon and women's accessory and specialty store. • After discovering the fraudulent charges, the cardholder properly disputed the charges and obtained a credit for the purchases. • The account was closed subsequent to the fraudulent activity.
4	Internet dating services Fraudulent card use	Various online dating services and pornographic sites	USPS	1,100	• Over a 15-month period, a postmaster used the government purchase card to subscribe to two Internet dating services. • The cardholder also used a government computer to access pornographic sites. • The dating service charges were the only charges on this card during our audit period, yet the activity went unnoticed by the agency for over 1 year. • The USPS Office of Inspector General conducted an investigation and issued a demand letter, and the cardholder paid restitution in full.
5	Airline ticket Fraudulent charge	Malev Hungarian Airlines	Department of State	890	• In supporting documentation provided to GAO, embassy officials stated that the airfare was fraudulently charged to the cardholder's account. • However, embassy officials could not provide evidence that the cardholder disputed the charge and that a credit was received. • An embassy official also stated that purchase reviews and approvals were not performed on a consistent basis during the time of the charge. • During the same period, the cardholder disputed and obtained credits for over $9,000 in other fraudulent charges. • The cardholder did not close the account until August 2006, when a second string of fraud occurred on this account.

Table 4. Fraudulent and Potentially Fraudulent Activity

(GAO, 2008, p. 23)

Case	Description of activity	Vendor	Agency	Amount	Additional facts
6	Multiple goods and services Fraudulent charges	Various vendors	Department of State	735	• Fraudulent charges appeared on the account, including for vendors such as Match.com, Old Navy–online, and AIPTEK (a camera and other electronic equipment manufacturer). • Upon discovery of the fraudulent charges, the cardholder appropriately followed agency procedures and contacted the purchase card bank, which closed the account.
7	Per diem Potentially fraudulent claim	Ritz Carlton Hotel	GSA	380	• GSA purchased continental breakfasts for 18 conference attendees for 3 days. • Sixteen of the 18 conference attendees claimed reimbursement for the breakfasts, which were provided by the government. Effectively, GSA paid for these meals twice. • Although the cardholder was authorized to purchase conference meals with the purchase card, the travelers submitted potentially fraudulent claim of $380—the amount that should have been deducted from the travelers' per diem. • In agency comments, GSA disagreed that continental breakfasts constituted full breakfasts, even when it paid $23 per person per day for this meal. Consequently, GSA plans to consult with other members of the travel community to decide on the treatment of continental breakfasts.
8	Meals Potentially fraudulent charges	Grape and Wine Conference	Alcohol and Tobacco Tax and Trade Bureau, Department of the Treasury	280	• In 2004 and again in 2006, the cardholder used the government card to purchase meals at two different conferences. • Although the cardholder did not claim reimbursement for the meals, the amounts he inappropriately charged to his purchase card well exceeded authorized meals and incidental expense amounts. • The agency did not discover these unauthorized purchases until a fiscal year 2006 audit review. • The cardholder repaid the agency in February 2007, over 2 years after the first unauthorized—and potentially fraudulent—purchase. • The cardholder received a written counseling letter and voluntarily turned in his purchase card, and the account was closed.

Table 5. Fraudulent and Potentially Fraudulent Activity
Source: (GAO, 2008, p. 24)

Case	Description of activity	Vendor	Agency	Amount	Additional facts
9	Per diem Potentially fraudulent claim	Radisson Hotel	GSA	150	• Five conference participants claimed reimbursement for meals that were provided by the government. • The cardholder was authorized to purchase conference meals with the purchase card; however, the traveler claimed full per diem for a dinner meal that had already been paid for with the purchase card.
10	Internet dating Compromised accounts	Match.com	Army	83	• Fraudulent charges appeared on the account in August 2005 for an Internet dating Web service. • The cardholder properly disputed the charge and obtained a credit in September 2005. • However, the account was still open as of September 2006, even though the standard practice in a case of fraudulent use of a card would be to close the account; the cardholder was still using the account a year later.

Source: GAO analysis, investigation, and review of purchase card data and supporting documentation.

The GAO (2002b) identified breakdowns in internal control activities that had major and serious consequences. Potentially fraudulent, improper, and abusive and questionable transactions went undetected due to inadequate or poor internal controls at several Army commands. The GAO notes that potentially fraudulent transactions include cardholder purchases that are intended for personal use and benefit, unauthorized transactions by vendors, or other purchases using compromised accounts (GAO, 2002b). As shown in Table 6, tens of thousands of dollars were spent on personal use items such as jewelry, computers, clothing, groceries, escort services, etc., by cardholders, approving officials, and other agency employees (GAO, 2002b). While these personal use purchases were identified at Army commands, unfortunately, this type of fraudulent and abusive behavior continues to happen across the military commands and installations, as well as civilian government agencies.

Table 6. Examples of Potentially Fraudulent Army Purchase Card Transactions
(GAO, 2002b, p. 44)

Type of items purchased	Where or how identified	Total amount	Individuals involved
Various items for personal use, such as computer game station, computer, digital camera, and surround sound system	Eisenhower Army Medical Center	$100,000 (estimated)	Cardholder, approving official, and others
Computer, rings, purses, and clothing from such vendors as Victoria's Secret, Calvin Klein, and others	Eisenhower Army Medical Center	30,000 (estimated)	Cardholder
Various items for personal use and cash advances	Fort Benning	30,000	Cardholder
Rental cars, cruises, cell phones, hotels, Payless Car Rental, Extended Stay America, and other vendors	Fort Benning	20,751	User of alleged stolen card
Car repairs, groceries, clothing, and other personal items	Eisenhower Army Medical Center	12,832	Cardholder and vendor
Personal clothing, trip to Las Vegas, payments of personal bills	Fort Benning	10,748	Cardholder
Sunglasses and other items for personal use from Sunglass Hut, Discovery Channel store, and others	Fort Hood	1,452	Separated cardholder, user of alleged compromised account
Various personal use items such as food and gas for personal vehicles at Shell and other vendors	Fort Benning	1,170	User of alleged stolen card
Digital camera from Office Max and other personal items from Circuit City and various other vendors	Fort Hood	786	Unknown
Escort services	Army-wide data mining	630	Cardholder
Prepaid phone cards from MCI, Sprint, and Ameritech, and pizza from Larry's Pizza and Po Boys	Fort Hood	524	Under investigation
Athletic shoes	Army-wide data mining	458	User of alleged compromised account
Internet site subscriptions	Fort Hood	210	Under investigation

Source: GAO analysis of Army purchase card transactions and related documentation.

After an audit of the Forest Service's government purchase card program, the GAO (2003) found that internal control weaknesses resulted in instances of improper, wasteful, and questionable purchases. As shown in Table 7, the GAO found various policy violations in the Forest Service's government purchase card program for FY2001. Of the total $1,628,299 in purchases identified as improper payments, split purchases accounted for $1,285,252 (GAO, 2003, p. 25).

Purchase cardholders use split purchase transactions to avoid exceeding the single purchase limit. Vendors comply with cardholders' requests to split or separate the purchases into several invoices to circumvent the single transaction limit. Single purchase limits are put in place so that any purchases above the established limits will be subject to additional controls, in order to ensure that the purchases are appropriately reviewed and approved before government funds are obligated. Unfortunately, GAO reports have found split purchases to be widely used by cardholders to avoid the purchase threshold, which is a violation of purchase card

policy. An effective monitoring system would help identify split purchases, as well as other types of improper purchases, such as unauthorized purchases and duplicate transactions (GAO, 2003).

Table 7. FY2001 Forest Service Purchase Card Program Categories of Improper Purchases
(GAO, 2003, p. 25)

Policy violation	Dollar amount of transactions
Split purchases	$1,285,252[a]
Duplicate transactions	177,187[b]
Purchases of unauthorized items	53,324
Purchases that exceeded single transaction limit	41,445
Information technology purchases that were not approved	25,452
Transactions on accounts of former employees	43,625
Convenience checks written for cash reimbursement	2,014
Total	**$1,628,299**

Source: GAO analysis of Forest Service purchase card and convenience check transactions selected for fiscal year 2001.

According to a DoD Inspector General (DoDIG) report in 2002, purchase card audits and investigations revealed incidents of abuse and fraud, citing causes to include inadequate command emphasis and poorly enforced internal controls (DoDIG, 2002). As a result of the highly publicized procurement fraud scandals, congressional leaders, such as Senator Charles Grassley, have called for more stringent oversight of government purchase card programs (Gupta & Palmer, 2007). On February 8, 2011, Senator Grassley and other co-sponsors introduced the Government Charge Card Abuse Prevention Act (2011), which calls for federal agencies to execute more stringent internal controls over purchase card usage.

The U.S. Agency for International Development (USAID) Office of Inspector General conducted an audit of the USAID government-wide commercial purchase card program and concluded that the USAID needed, among other things, to improve the following (DoDIG, 2002):

1. Controls to Safeguard Purchase Cards

2. Documentation of Purchase Card Approval and Usage

3. Controls over the Segregation Of Duties

4. Training of Cardholders and Approving Officials

5. Oversight of Its Purchase Card Program

When the DoD Inspector General (2007) investigated internal controls over the Army, Navy, and Air Force purchase card programs, it found that purchase card program officials at various military installations failed to establish and implement effective controls and oversight over their government purchase card programs. Furthermore, internal controls over purchase card program training at two of the three Navy installations visited were found to be weak and inadequate (DoDIG, 2007).

At the Defense Procurement Director's request, the DoD Office of Inspector General prepared a summary report of purchase card audit report findings that identified misuse trends and problem areas in the government purchase card program (DoD, 2001).

Of the 382 reports that were issued on the DoD government purchase card program from FY1996 through FY2001, Table 8 outlines the federal government agencies and the number of reports that were issued during that timeframe (DoD, 2001).

Table 8. Summary of Federal Agency Reports Issued on Government Purchase Card Programs FY1996 to FY2001
(DoD, 2001)

Federal Agency	Number of Reports Issued
General Accounting Office	3
DoD Inspector General	3
Army Audit Agency	32
Naval Audit Service	1
Air Force Audit Agency	255
Defense Agencies Inspector General & Internal Review Offices	27
Army Internal Review Office	61

The systemic issues that were identified in the reports that were issued between FY1996 and FY2001 on government purchase card programs included the following:

- Account Reconciliation and Certification (88 reports),
- Administrative Controls (70 reports),
- Management Oversight (115 reports),
- Property Accountability (79 reports),
- Purchase Card Use (50 reports),
- Purchases (222 reports),
- Separation of Duties (22 reports), and
- Training (52 reports). (DoD, 2001)

The GAO reports and Inspector General reports that were reviewed show a common thread throughout. The overarching issues found in many of the improper, abusive, and fraudulent activities have been related to the lack of properly implemented internal controls and oversight of government purchase card programs. These incidents of inappropriate behavior within the government purchase card programs can be reviewed for commonalities in terms of potential fraud indicators.

The following section will discuss potential fraud indicators in government purchase card programs.

C. Fraud Indicators In Government Purchase Card Programs

When DoD auditors are determining the fraud indicators and risk factors involved in a case, they should not merely take into consideration the materiality or monetary impact, but should also consider other important non-quantitative aspects, such as the safety and welfare of service members and civilians. If DoD auditors find fraud indicators or risk factors that relate to such qualitative factors, a significantly lower threshold should be used for categorizing an area as high risk. DoD auditors are expected to uphold their fiduciary duties and responsibilities to the Department of Defense, the U.S. government, and the public (DoDIG, 2011).

Potential indicators of fraudulent activity are clues or red flags that warrant a closer investigation into a certain area or activity. Intent is the key determining factor as to whether a particular situation is deemed fraud or mere negligence. The DoD Inspector General's website provides fraud guidance for their auditors, citing numerous, but not all-inclusive, possible purchase card fraud indicators. As outlined in Table 9, some possible purchase card fraud indicators include, but are not limited to, inadequate separation of duties such as cardholders approving their own purchase authorizations, cardholder and vendor having the same name, and similar invoices coming from different vendors (DoDIG, 2011). Many of the policies and procedures that would address many of these issues are included in the DoD purchase card program handbook.

Table 9. Purchase Card Fraud Indicators
(DoDIG, 2011)

Purchase Card Fraud Indicators
• Numerous missing invoices, receipts, and purchase justifications are noticed.
• Receipts contain —white-outs," date changes, and changes to product descriptions.
• Purchased items are not recorded in inventory records.
• Pattern of repeat favoritism to a specific vendor or group of vendors is seen.
• Purchases fall at, or slightly below, the purchase threshold of $3,000.
• Independent receipt and acceptance of purchased items are missing.
• Organization does not conduct periodic reviews of cardholder purchases and inventory.
• One cardholder, or a small number of cardholders, makes repeat purchases from a specific vendor.
• Research shows that a vendor or company may not be authentic (i.e., phony business address, or no evidence that the company is incorporated, etc.); fictitious vendor.
• Management does not follow established purchase card procedures such as requiring purchase justifications, independent receipt and acceptance of purchased items, and periodic reviews of cardholder transactions.
• Cardholder makes unauthorized weekend purchases.
• Cardholder pays an excessive amount for routine purchases.
• Pattern of suspect cardholder purchases from unauthorized vendors such as clothing stores or suspect online vendors is detected.
• Pattern of cardholder accounts with disputed charges is noted.
• Purchase logs do not contain descriptions of items purchased.
• Pilferable items are repeatedly reported as lost, missing, or stolen.

- Inadequate separation of duties, such as cardholders approving their own purchase authorizations, is found.
- Cardholder and vendor have the same name.
- Cardholder account records are incomplete.
- Cardholder accounts with several limit increases occur within a short time.
- Cardholder purchases exceed the authorized card limit.
- Purchases appear to be outside of the normal purchase pattern of the cardholder.
- Similar invoices from different vendors are found.
- Subversion of management controls by the cardholder and/or approving authority is detected.
- Excessive number of cardholders is within an activity or unit.
- Purchased items are available through the supply system.
- Cardholder does not turn in premiums/free products obtained with purchases.
- Organization has no established controls over purchases returned to stores for cash.
- Purchase card assigned to an office or group of individuals instead of a specific person.
- An excessive number of cardholders are assigned to one approving official.
- Separated employees continue to make purchases using the government purchase card.

In addition, the Air Force Audit Agency's (AFAA) handbook on fraud and waste indicators defines fraud as —an illegal act where one obtains something of value through willful misrepresentation" (Air Force Audit Agency, 1997, p. 1). The AFAA handbook outlines the following common elements that exist in fraudulent activities:

1. Intent—willfully committing a wrongful act which must be proven through a pattern of activity, such as repeated engagement in the wrongful activity or making conflicting statements.

2. Disguise of Purpose—misrepresentations made to accomplish the scheme when representations are made that were false by either omission or commission.

3. Reliance—the offender knowingly makes a misrepresentation that is relied upon and acted upon by the victim.

4. Voluntary—the victim assists the offender; for example, in a case of employee theft, the victim (the Air Force) entrusted the care of assets to the offender, which established a fiduciary capacity.

5. Concealment—hiding or preventing knowledge of the fraudulent activity.

6. Injury or Damage—the victim (the Air Force) suffers a loss of money or property because he/she relied and acted upon the misrepresentation. (Air Force Audit Agency, 1997, pp. 1–2)

Red flags or fraud indicators can be categorized into situational and opportunity red flags for either personal gain or for organizational benefit, and personal characteristics red flags, which include low moral character, wheeler-dealer attitude, rationalization of contradictory behavior, poor credit rating or financial status, and lack of stability (Air Force Audit Agency, 1997, pp. 4–7). Table 10 shows examples of situational red flags or fraud indicators, which include such things as living beyond one's means or inadequate income or greed, for personal gain; and urgent need for favorable performance or temporary bad situation, for organization benefit. Table 11 shows examples of opportunity red flags or fraud indicators, such as close association with suppliers and key people, or too much trust in key employees, for personal gain; and poor internal controls or related party transactions, for organizational benefit. It should be noted that these fraud indicators are merely an indication of possible fraudulent activities; they do not guarantee that actual fraudulent activities are taking place (Air Force Audit Agency, 1997).

Table 10. Situational Red Flags/Fraud Indicators
(Air Force Audit Agency, 1997, p. 4)

For Personal Gain	For Organizational Benefit
High personal debt or losses	Heavy expenditures
Living beyond one's means	Urgent need for favorable performance
Gambling or speculation	Revoked or imperiled mission status
Excessive use of alcohol or liquor	Unfavorable economic conditions
Perceived inequities in the organization	Temporary bad situation
Resentment of supervisors	Insufficient working capital/equipment
Inadequate income or greed	Obsolete inventories/production assets

Table 11. Opportunity Red Flags/Fraud Indicators
(Air Force Audit Agency, 1997, pp.5-6)

For Personal Gain	For Organizational Benefit
Familiarity with operations and position of trust	Related party transactions
Close association with suppliers and key people	Poor accounting records
Dominant top management	Poor internal controls
Dishonest or unethical management	Inexperienced people in key positions
Too much trust in key employees	Reluctant to give auditors needed data
Rapid turnover of key employees	Continuous problems with inspectors
Inadequate training programs	Highly computerized organization
Weak or dishonest personnel evaluations	Inadequate staffing in critical positions

According to the National Association of Purchasing Card Professionals (NAPCP), the use of purchase cards (P-cards) can save as much as 50% in processing costs versus using an organization's normal procurement process. However, when the purchase card privileges are abused, and unauthorized or

fraudulent purchases are made, any cost efficiencies gained through the use of the P-card may end up being lost (Goldmann, 2011). P-card fraud is one type of procurement fraud that threatens organizations across all industries, especially during a tough economy. Some P-card red flags identified by Goldmann (2011) include the following:

- P-cards are used for unusual purchases unrelated to the business;
- An unusual number of purchases are made for amounts just below the organization's minimum threshold amounts which require management approval;
- Photocopied receipts are submitted with expense reports instead of original receipts;
- Split payments are made for purchases, which may be an indicator of attempts to circumvent purchase limit rules; and
- Receipts for purchases are forged.

Other general red flags that could lead to fraudulent activities that were identified by various GAO reports and OIG audits include the following (DoDIG, 2011):

- Management override of key controls,
- Inadequate or weak internal controls,
- No written policies and procedures,
- Overly complex organizational structure,
- Key employee never taking leave or vacation,
- High turnover rate, reassignment, firing of key personnel,
- Missing electronic or hard copy documents that materialize later in the review,
- Lost or destroyed electronic or hard copy records,
- Photocopied documents instead of originals; Copies are poor quality or illegible,

- —bofficial" electronic files or records instead of —archived" or "official" files or records,
- Revisions to electronic or hard copy documents with no explanation or support,
- Computer-generated dates for modifications to electronic files that do not fit the appropriate time line for when they were created,
- Missing signatures of approval or discrepancies in signature/handwriting,
- Computer report totals that are not supported by source documentation, and
- Lengthy unexplained delays in producing requested documentation.

The GAO defines potentially fraudulent purchases as those that are unauthorized and intended for personal use (GAO, 2002a). Furthermore, government auditors use data mining techniques to help identify suspicious purchase card transactions by reviewing unusual or questionable transactions, such as those that occur on weekends, purchases from unauthorized vendors, split purchases, and purchases slightly below the $3,000 threshold for micro-purchases. Data mining is a computer-based tool that is used by auditors to sort through numerous amounts of data to pick out relevant information and reveal patterns (DoDIG, 2011).

The myriad of fraud indicators identified in this research provide an overall foundation for the types of behavior and/or situations that could either lead to fraudulent use of government purchase cards, or point to ongoing fraudulent activities by government officials within the government purchase card programs agency-wide. As shown in the lists of fraud indicators identified, and in the fraudulent activities by government officials in the government purchase card programs, one of the common threads in many of these situations is a lack of properly implemented strong internal controls. The following section will discuss government purchase card program internal control issues.

D. Government Purchase Card Program Internal Control Issues

1. The Sarbanes-Oxley Act of 2002 and Internal Controls

The importance of transparency, trust, and confidence in government governance cannot be overemphasized. The U.S. Congress, in response to public accounting failures, enacted the Sarbanes-Oxley Act of 2002 (~~t~~the Act") in efforts to deter fraudulent activities (Latshaw, 2003; Marden & Edwards, 2005). The Act revised the regulation of accounting firms that audit public companies, transformed corporate reporting and enforcement, and included internal control requirements for publicly traded companies (Lander, 2004). Section 404 of the Act outlines the legislative requirements for internal controls for publicly traded companies (Sarbanes-Oxley Act, 2002). While the Act's internal control requirements are for publicly traded companies, the components of internal controls are just as important in the federal government, specifically in the government purchase card programs agency-wide. As the GAO reports and IG audits indicate, internal control violations eroded the efficiency of controls over the management of government purchase card programs, which resulted in fraudulent activities (GAO, 2008). The next section will discuss the internal control framework.

2. Internal Control Framework

In compliance with the Federal Managers' Financial Integrity Act (FMFIA) (1982) requirement, the General Accounting Office (GAO) developed relevant updated internal control guidance based on the private sector's Internal Control–Integrated Framework, which is published by the Committee of Sponsoring Organizations of the Treadway Commission (Whittington & Pany, 2012). Furthermore, the Chief Finanical Officers Act (1990) noted that billions of dollars were being lost each year through fraud, waste, abuse, and mismanagement, and cited that these losses could be significantly reduced with improved management, internal controls, and financial accounting. In addition, the Federal Financial Management Improvement Act (1996) identified internal control as an important and

integral component of improving financial management systems. Therefore, in 1999, the GAO issued —Standards for Internal Controls in the Federal Government" to assist government managers in achieving their missions and program results, and in improving accountability (GAO, 1999).

Internal control is defined as a process designed to provide reasonable assurance regarding the achievement of objectives in the following categories: (1) reliability of financial reporting, (2) effectiveness and efficiency of operations, and (3) compliance with applicable laws and regulations. The components of the internal control framework include the following (Whittington & Pany, 2012):

1. The Control Environment,
2. Risk Assessment,
3. The Accounting Information System,
4. Control Activities, and
5. Monitoring.

In a 2001 memorandum to the Assistant Secretary of the Army (Acquisition, Logistics, and Technology), Assistant Secretary of the Navy (Research, Development, and Acquisition), Assistant Secretary of the Air Force (Acquisition), and directors of defense agencies, Bruce Sullivan, Director of the Purchase Card Joint Program Management Office, emphasized the need to allocate the appropriate resources necessary to have a system of internal and management controls in place that will help ensure the appropriate management of fraud related losses in order to protect the interests of the American public. He also addressed the issue of an appropriate span of control for billing officials, citing 5–7 cardholders per billing official as a general rule of thumb (Sullivan, 2001).

Per the *Standards for Internal Control in the Federal Government*, internal control activities, such as authorizations, verifications, reconciliations, and documentation, are essential in helping to ensure that management's directives are accomplished (GAO, 2008).

Gillett, Fink, and Johnson (1997) note that government agencies must implement proper internal controls to make sure that correct information is recorded and maintained, so that government purchases can be analyzed and reviewed in a timely manner. A serious breakdown in internal controls over purchase card programs can leave government agencies vulnerable to purchase card fraud and abuse (GAO, 2001). When government employees, such as cardholders and approving officials, overstep the boundaries of internal controls and established policies and procedures with a self serving interest at the expense of the American people, sustained public confidence in the procurement system is jeopardized. The increased fraud vulnerability due to lack of proper implementation of internal controls within the GPCPs, threatens the public's trust in the procurement process.

Colaianni (2005) believes that some internal controls that were implemented by the U. S. Department of State could prove useful in other GPCPs. She advocates the establishment of individual card dollar limits and the use of merchant category code restrictions. The enforcement of basic and refresher training and implementation of online training programs reduced administrative costs and increased procedure consistency at the Department of State. The identification of individual responsibilities and oversight and reporting requirements can also help improve GPCPs, such as developing a standardized checklist or template to assist employees with requirements. In addition, the enforcement of annual program performance reviews assists in improving management oversight and increasing compliance with purchase card program requirements (Colaianni, 2005).

After purchase card program audits and investigations revealed incidents of purchase card abuse, misuse, and fraud within the DoD, the Secretary of Defense called for a review of the government purchase card programs, also known as charge card programs. A DoD Charge Card Task Force, which included representatives from major defense organizations, was established to evaluate the DoD's purchase card programs and develop recommendations for improvement (DoD, 2002).

The task force focused on three major areas of investigation that included management emphasis and organizational culture, compliance, and process and workforce development. Even though the task force's findings concluded that most DoD's military and civilian personnel properly use purchase and travel charge cards and utilize appropriate fiscal stewardship of taxpayer dollars, they found that major problems do exist in government-wide purchase card programs. Some of the issues identified in the investigation included weak and unenforced internal controls, inadequate command emphasis of proper purchase card conduct, and lack of personal accountability (DoD, 2002).

In order to significantly improve the DoD's charge card programs, the task force made various recommendations which included increasing management emphasis on ethical conduct and personal accountability, strengthening internal controls and increasing the tools available to managers for enforcing those controls in efforts to detect fraudulent or abusive charge card transactions, and enhancing the capability of government employees to accomplish their assigned charge card responsibilities through proper training (DoD, 2002).

The GAO found internal control weaknesses for Army, Navy, and Air Force purchase card programs as defined by DoD Instruction 5010.40, —Managers' Internal Control (MIC) Program Procedures" (GAO, 2003; DoD, 2010). GAO (2002b) found that weak internal controls in the government purchase program leave the Army highly vulnerable to potentially fraudulent, improper, and abusive purchases. Informal and incomplete operating procedures, as well as ineffective oversight of the purchase card program, were cited as two major contributors to the weak overall control environment at several Army commands. While the Army commands had established policies and procedures, they were inconsistent between commands and provided inadequate internal control guidance, which resulted in a high failure rate between 40%– 86% for the control activity of approving official reviews, and resulted in potentially fraudulent transactions going undetected due to serious breakdowns in internal control (GAO, 2002b).

In January 2007, an audit by the DoD Inspector General on the government purchase card programs of several military agencies resulted in a determination that GPCP officials need to strengthen their internal controls and proper program oversight in order for the Army, Navy, and Air Force to ensure continuous program improvement and risk mitigation essential for preventing fraud, waste, or mismanagement (DoDIG, 2007).

Federal government officials, such as GPCP approving officials and cardholders, hold a public trust and are expected to meet the highest ethical standards, especially when working with millions of taxpayer dollars on behalf of the American people. Because fraud is a serious problem throughout the nation and for the public procurement arena, it is crucial that procurement officials receive the appropriate training and learn the skills necessary to deter and detect fraud within agency-wide Government Purchase Card Programs. Unfortunately, many government executives have failed to implement and follow the existing internal control policies that are in place to help deter and detect fraudulent activities (GAO, 2008). Financial management transparency could be a significant and powerful fraud deterrent, and as Wells (2004) points out, occupational fraud is affected by the integrity level of government leaders and employees, and the perception of detection. The following section will provide a summary and conclusion.

II. Recommendations

Many federal executives recognize the potential benefits that could result from the use of purchase cards; however, many are also concerned about the increased potential for fraudulent, abusive, and wasteful spending. The rampant wave of incidents of fraud, waste, and abuse found by the GAO and various Offices of Inspectors General, both in the civilian, as well as in the military agencies and organizations, have played a role in the decreasing number of cardholders throughout the years.

What needs to be addressed in any analysis of the purchase card programs is the fact that incidences of purchase card fraud, abuse, and misuse involve taxpayer dollars—dollars that belong to the American people. Taxpayers should not be footing the bill for fraudulent and abusive purchases. There is still a debate between federal employees who want to improve government efficiency with little or no regard for the misuse of government purchase cards, and those who are seriously concerned about fraud, abuse, and misuse of the government purchase card. The fraudulent exploitation of taxpayer resources is a major issue and is a public interest that should not be taken lightly. Every dollar that is fraudulently spent takes away from funds that could be spent on goods and services that are needed by federal agencies to meet their missions in support of the overall goal of public service to the American people.

Agency executives need to establish and implement purchase card policies that instill integrity, transparency, and accountability in their purchase card programs. The shift from low-value paper transactions to the purchase card was intended to save taxpayers money and eliminate the paperwork involved in the procurement process for micro-purchases, not to give federal government employees free reign of taxpayer funds for personal use.

Margaret A. Colaianni, the purchase card program manager of the Department of State, provides useful recommendations that could be implemented

in other government purchase card programs. Colaianni (2005) believes that the three fundamental principles for the Department of State purchase card program--standardization, centralization, and collaboration--could be helpful in other federal agencies' government purchase card programs.

Some best practices surfaced from the three underlying principles she identified that could assist agencies in meeting the challenges and demands of managing government purchase card programs. For example, she recommends that agencies standardize practices as much as possible, such as in the areas of cardholder purchasing logs, procedures, guidance, and practices. Standardized processes can help in the reduction of the administrative burden, the improvement of reconciliation procedures, the cutback of costs, and the decrease in processing times (Colaianni, 2005).

Implemented as a cost-savings initiative to improve purchase processes and mission effectiveness, over the years, the DoD purchase card program has proven to be valuable, yet also vulnerable to abuse and fraud. While purchase cards come with an inherent risk of abuse, misuse, and fraud, GAO reports and DoDIG audit reports of purchase card programs government-wide show evidence of failures of the internal controls designed to alleviate that inherent risk. Furthermore, these types of failures cultivate the misperception that the Department of Defense is not able to effectively and efficiently manage the public resources with which it is entrusted (DoD, 2002).

Colaianni (2005) believes that collaboration among team members, as well as with other agencies, participating banks, and the credit card associations, is vitally important. Sharing best practices and strategies that work in the management of government purchase card programs is essential to the long-term success of any government purchase card program. She also recommends collaboration, such as establishing a close working relationship between the purchasing and finance office that pays the invoices, and establishing written operating procedures at the local level, in addition to the agency-wide guidance and procedures. Furthermore, she

suggests keeping program and hierarchy information updated to account for any employee turnover, as well as keeping cardholders' established profile parameters current (Colaianni, 2005).

As noted previously, in efforts to significantly improve the DoD's charge card programs, the DoD Charge Card Task Force made various recommendations, which included increasing management emphasis on ethical conduct and personal accountability, strengthening internal controls and increasing the tools available to managers for enforcing those controls in efforts to detect fraudulent or abusive charge card transactions, and enhancing the capability of government employees to accomplish their assigned charge card responsibilities through proper training (DoD, 2002). Merely having established internal control policies without implementing those policies is like not having any internal control policies in place at all. The following section will provide a summary and conclusion.

THIS PAGE INTENTIONALLY LEFT BLANK

III. Summary & Conclusion

This research explored the Department of Defense (DoD) Government Purchase Card Program. The specific purpose of this research was to identify fraud indicators within the DoD GPCPs. This research identified fraud indicators within the DoD GPCPs and provided recommendations for improving the management of GPCPs within the DoD. First, a brief background of the DoD GPCP was provided. Second, based on GAO reports and OIG audits, incidents of procurement card fraud were discussed. Third, fraud indicators in the GPCPs were identified. Fourth, GPCP internal control issues were addressed. In addition, areas for further research were discussed.

The government purchase card program's main goal was to provide federal agencies with an efficient way to purchase goods and services directly from vendors or suppliers (DoD, 2002). Even though purchase cards streamline the federal procurement process, the GAO reports since 2001 have shown that, if not managed and controlled appropriately, the use of government purchase cards can result in fraud, waste, and abuse (GAO, 2008). In light of all the recent federal procurement scandals, the emergence of additional guidance for GPCPs has been steadily increasing. The more approving officials and cardholders are aware of perceived weaknesses in internal controls, the more likely they will be to take appropriate steps to reduce the potential for fraudulent activities.

Over the last several years, the GAO has issued various reports and testimonies on the purchase card programs of different government agencies resulting in serious findings of fraudulent, improper, and abusive activities. These types of findings severely undermine the credibility of the GPCP (GAO, 2008). The federal government, in the face of severe fiscal challenges, spends billions of dollars annually through its purchase card programs. Therefore, federal employees, such as cardholders, approving officials, and GPC program managers, who hold a position of public trust, should maintain stewardship over the federal funds at their

disposal, follow appropriate acquisition requirements, and ensure that purchase cards are being used responsibly (GAO, 2008).

While Gupta and Palmer (2007) agree that the incidents of purchase card fraud, abuse, and misuse found by the GAO and various Offices of Inspectors General are unacceptable, they also believe that there could be a significant opportunity cost associated with an under-used purchase card program. Therefore, government officials need to have a balanced approach to managing their GPCPs. As the U.S. government faces increased buying of commodities and services with less acquisition and finance personnel, the SmartPay program's accomplishments to date have positioned it to continue improving the GPCP.

The government needs to make sure that it spends the American taxpayers' dollars wisely, efficiently, and effectively. It must find ways to reduce fraud, waste, and abuse. It is imperative that purchasing transactions result in the best value for the American taxpayer. The following section discusses areas for further research.

IV. Areas for Further Research

The recent GAO reports and IG audits have shown that there is a need for research in the area of procurement fraud in the GPCP (GAO, 2008). The focus of this research was to identify fraud indicators that could be used by DoD agencies to improve purchase card programs. Other research that could be done would be to expand on the identified fraud indicators and lead to the development of an assessment tool to be used in the identification of procurement fraud vulnerabilities in the GPCP. In addition, an analysis by specific government agencies such as the Navy, Air Force, and Army would be recommended.

THIS PAGE INTENTIONALLY LEFT BLANK

References

Air Force Audit Agency. (1997, December 1). *Audit agency handbook 65-109: Fraud and waste indicators.* Retrieved from http://www.dodig.mil/Inspections/APO/fraud/AFAAFraudHandbook.pdf

American Psychological Association. (2010). *Publication manual of the American Psychological Association* (6th ed.). Washington, DC: Author.

Chief Financial Officers Act, Pub. L. No. 101-576, § 102, 104 Stat. 2838 (1990, November 15). Retrieved from http://www.cfoc.gov/documents/PL101-576.pdf

Colaianni, M. A. (2005). Principles and practices of managing a global purchase card program. *Journal of Public Procurement, 5*(1), 88–93. Retrieved from http://ippa.org/jopp/download/vol5/issue-1/PractitionerCorner_Article.pdf

Defense Acquisition University (DAU). (2010). *DoD purchase card program course CLG 001*. Retrieved from https://learn.dau.mil/html/clc/course/CourseLaunch.jsp?course_id=801402&clcid=C00105&course_prefix=CLG&version=5&scorm_version=3&roster_id=-1_801402&course_name=DoD Government Purchase Card&mode=normal&course_number=001&mode_id=10&course_suffix=

Defense Federal Acquisition Regulation Supplement (DFARS), 48 C.F.R. Part 213. (1999, Janurary 15). *DFARS Simplified Acquisition Procedures*. Retrieved from http://www.acq.osd.mil/dpap/dars/dfars/changenotice/docs/97d306.txt

Defense Procurement and Acquisition Policy (DPAP). (2011). *Defense procurement and acquisition policy*. Retrieved from http://www.acq.osd.mil/dpap/

Department of Defense (DoD). (2001, December 27). *Summary of DoD purchase card program audit coverage* (Report No. D-2002-029(PDF)-Project No. D2001PA-0185.000). Retrieved from http://www.dodig.mil/Audit/reports/fy02/02029sum.htm

Department of Defense (DoD). (2002, June 27). *Department of Defense (DoD) Charge Card Task Force final report*. Retrieved from http://comptroller.defense.gov/charge_card_tf_final.pdf

Department of Defense (DoD). (2009, April 30). *Department of Defense government charge card guidebook for establishing and managing purchase, travel, and fuel card programs*. Retrieved from http://www.acq.osd.mil/dpap/pcard/pcardguidebook.pdf

Department of Defense (DoD). (2010a, August). Internal management controls. In *DoD Financial Management Regulation* (Vol. 5). Retrieved from http://comptroller.defense.gov/fmr/05/05_01.pdf

Department of Defense (DoD). (2010b, September). Introduction. In *DoD Financial Management Regulation*. Retrieved from http://comptroller.defense.gov/fmr/intro.pdf

Department of Defense (DoD). (2010c, September). 10 U.S.C., § 2784(b)(8). *Summary of major changes to DoD 7000.14-R, purchase card payments*. In *DoD Financial Management Regulation* (Vol. 10). Retrieved from http://comptroller.defense.gov/fmr/10/10_23.pdf

Department of Defense (DoD). (2010d, December). Smart cards for financial applications. In *DoD Financial Management Regulation* (Vol. 5). Retrieved from http://comptroller.defense.gov/fmr/05/05_17.pdf

Department of Defense Inspector General (DoDIG). (2002, March 19). *Audit of USAID's governmentwide commercial purchase card program audit report* (Number 9-000-02-004-P). Retrieved from http://www.ignet.gov/randp/cards/usaid-9-000-02-004-P.pdf

Department of Defense Inspector General (DoDIG). (2007, January 10). *Report on controls over the Army, Navy, and Air Force purchase card programs* (Report No. D-2007-043). Retrieved from http://www.dodig.mil/Audit/reports/FY07/07-043.pdf

Department of Defense Inspector General (DoDIG). (2011). *Purchase card fraud indicators*. Retrieved from http://www.dodig.mil/inspections/apo/fraud/scenarios_pdfs/PurchaseCards.pdf

Exec. Order No. 11541, 3 C.F.R. 939 (1970). Retrieved from http://www.archives.gov/federal-register/codification/executive-order/11541.html

Federal Acquisition Regulation (FAR), 48 C.F.R. Part 13 (2011, April 1). *Simplified Acquisition Procedures*. Retrieved from http://farsite.hill.af.mil/reghtml/regs/FAR2AFMCFARS/FARDFARS/FAR/13.htm#P0_0

Federal Financial Management Improvement Act of 1996 (FFMIA). 31 USC § 3512. Pub. L. No. 104-208, § 802, 110 Stat. 3009. (1996, September 30) Retrieved from www.dol.gov/ocfo/media/regs/FFMIA.pdf

Federal Managers' Financial Integrity Act of 1982 (FMFIA). 31 USC § 3512. Pub. L. No. 97-255. (1982, September 8). Retrieved from http://www.whitehoures.gov/omb/financial_fmfia1982

Financial Management Services (FMS). (2010). *Treasury financial manual for guidance of departments and agencies* (TFM 4-4500). Retrieved from http://www.fms.treas.gov/tfm/vol1/v1p4c450.txt

Fischer, D. (2006, May). A growing method of payment evolves online. *Contract Management, 46*(5), 42–48.

General Services Administration (GSA). (2011a). GSA SmartPay. Retrieved from http://www.gsa.gov/portal/content/104616

General Services Administration (GSA). (2011b). GSA SmartPay program fiscal year 2010 executive summary. Retrieved from https://smartpay.gsa.gov/sites/default/files/wysiwyg/2010%20Executive%20Summary.pdf

General Services Administration (GSA). (2011c). GSA SmartPay statistics. Retrieved from https://smartpay.gsa.gov/about-gsa-smartpay/program-statistics

General Services Administration (GSA). (2011d). Office of charge card management. Retrieved from http://www.gsa.gov/portal/content/105080

Gillett, J. W., Fink, R. L., & Johnson, L. T. (1997, December). Accounting controls in a procurement card environment. *Management Accounting, 79*(6), 47–51.

Goldmann, P. (2011, March). Procurement fraud: How to protect against this often-underestimated threat. Retrieved from the Association of Certified Fraud Examiners website: http://www.acfe.com/newsletters/fraud-examiner.asp?copy=march11-goldmann-column

Government Accountability Office (GAO). (1996, August 6). *Acquisition reform: Purchase card use cuts procurement costs, improves efficiency* (GAO/NSIAD-96-138). Retrieved from http://www.gao.gov/archive/1996/ns96138.pdf

Government Accountability Office (GAO). (1999, November). *Standards for internal control in the federal government* (GAO/AIMD-00-21.3.1). Retrieved from http://www.gao.gov/special.pubs/ai00021p.pdf

Government Accountability Office (GAO). (2001, July 30). *Purchase cards: Control weaknesses leave two Navy units vulnerable to fraud and abuse* (GAO-01-995T) [Testimony]. Retrieved from http://www.gao.gov/new.items/d01995t.pdf

Government Accountability Office (GAO). (2002a, May 1). *Government purchase cards: Control weaknesses expose agencies to fraud and abuse* (GAO-02-676T). Retrieved from http://www.gao.gov/new.items/d02676t.pdf

Government Accountability Office (GAO). (2002b, June). P*urchase cards: Control weaknesses leave Army vulnerable to fraud, waste, and abuse* (GAO-02-732). Retrieved from http://www.gao.gov/new.items/d02676t.pdf

Government Accountability Office (GAO). (2003, August). *Forest service purchase cards: Internal control weaknesses resulted in instances of improper, wasteful, and questionable purchases* (GAO-03-786). Retrieved from http://www.gao.gov/new.items/d03786.pdf

Government Accountability Office (GAO). (2008, March). *Governmentwide purchase cards: Actions needed to strengthen internal controls to reduce fraudulent, improper, and abusive purchases* (GAO-08-333). Retrieved from http://www.gao.gov

Government Charge Card Abuse Prevention Act of 2011, 112th Cong. § 300 (2011). Retrieved from http://www.govtrack.us/congress/bill.xpd?bill=s112-300

Gupta, M., & Palmer, R. (2007, Summer). Purchase card use by the U.S. government: Growth and future opportunity. *Journal of Government Financial Management, 56*(2)*, 24–31.*

Kozaryn, L. D. (2002, March 27). *DoD fights government credit card abuse*. Washington, DC: American Forces Press Service.

Lander, G. P. (2004). *What is Sarbanes–Oxley?* New York: McGraw Hill.

Latshaw, C. A. (2003, Spring). Fraudulent financial reporting: The government and accounting profession react. *Review of Business, 24*(2)13–15.

Marden, R., & Edwards, R. (2005, April). The Sarbanes–Oxley ax. *The CPA Journal*, *75*(4), 6–9.

Mills, T. H., Normand, C. J., & Palmer, R. J. (2008). Governmental purchase card programs: A case on the stewardship of public resources. *Accounting Perspectives*, *7*(1), 69–81.

Office of Management and Budget (OMB). (2009, January 15). *Improving the management of government charge card programs* (Appendix B, Rev. ed.; OMB Circular A-123). Retrieved from http://www.whitehouse.gov/sites/default/files/omb/circulars/a123/a123_appendix_b.pdf

Palmer, R. J., Gupta, M., & Dawson, R. (2010). U.S. government use of commercial card technology: A case for change in military card distribution policy. *Defense AR Journal, 17*(3), 313. Retrieved from http://search.proquest.com/docview/722555622?accountid=12702

Sarbanes-Oxley Act of 2002, H.R. 3763, 107 P.L. 204, Title IV, § 404, 116 Stat.745. (2002, July 30). Retrieved from http://taft.law.uc.edu/CCL/SOact/sec404.html

Struebing, L. (1996, December). Credit card use cuts procurement costs and improves efficiency. *Quality Progress, 29(*12), 14.

Sullivan, B. (2001, July 5). *Internal and management controls—DoD purchase card program* [Memorandum]. Retrieved from http://dodgpc.us.army.mil/Management%20Controls.pdf

Under Secretary of Defense (Comptroller). (2010, July 29). *Managers' Internal Control Program (MICP) procedures* (DoD Instruction 5010.40). Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/501040p.pdf

Wells, J. T. (2004, February). New approaches to fraud deterrence. *Journal of Accountancy*, *197*(2), 72–76.

Whittington, O. R., & Pany, K. (2012). *Principles of auditing and other assurance services* (18th ed.). New York, NY: McGraw–Hill Irwin.

THIS PAGE INTENTIONALLY LEFT BLANK

Initial Distribution List

1. Defense Technical Information Center 2
   8725 John J. Kingman Rd., STE 0944; Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library, Code 013 2
   Naval Postgraduate School, Monterey, CA 93943-5100

3. Research Office, Code 09 1
   Naval Postgraduate School, Monterey, CA 93943-5138

4. William R. Gates 1
   Dean, GSBPP
   Naval Postgraduate School, Monterey, CA 93943

5. Stephen Mehay 1
   Associate Dean for Research, GB
   Naval Postgraduate School, Monterey, CA 93943

6. Juanita M. Rendon 1
   Lecturer, GB
   Naval Postgraduate School, Monterey, CA 93943

Copies of the Acquisition Sponsored Research Reports may be printed from our website: www.acquisitionresearch.org