

2012

Prepared for the DoD  
Purchase Card  
Policy Office

Version 2.0

June 2012



# Department of Defense Micro-Purchase & Purchase Card Data Management Plan

TABLE OF CONTENTS

1.0 Overview ..... 1

    1.1 Document Overview ..... 2

    1.2 Document Scope ..... 2

    1.3 Document Vision..... 3

2.0 Government Purchase Card Data Flow..... 4

    2.1 GPC Account Request and Issue Process Overview ..... 4

        2.1.1 Request and Issue Data Flow ..... 5

        2.1.2 Request and Issue Data Capture and Retention..... 6

    2.2 Card Use Process Overview..... 7

        2.2.1 GPC Account Use Data Flow ..... 7

        2.2.2 GPC Account Use Data Capture and Retention..... 9

    2.3 Usage Visibility and Oversight ..... 11

        2.3.1 Purchase Card Billing Data ..... 12

        2.3.2 Data Mining / Risk Assessment Data ..... 14

        2.3.3 Wide Area Workflow Data ..... 17

        2.3.4 Federal Procurement Data System Data ..... 19

    2.4 Post Use Review ..... 19

    2.5 Business Intelligence ..... 22

    2.6 PCOLS Business Intelligence ..... 23

    2.7 Office of Management and Budget (OMB) Reporting ..... 25

3.0 Data, Process Standardization, and Security ..... 26

    3.1 DoD EMALL..... 26

    3.2 DoD 3-in-1 Tool ..... 27

4.0 Summary ..... 29

    4.1 Summary of Actions..... 29

Appendix A: Overview of DEF/VCF File Structure ..... A-1

Appendix B: AF NAF Reconciled Data Format ..... B-1

Appendix C: Bank Extract File Comparison to RPM ..... C-1

Appendix D: Risk Predictive Model Daily File ..... D-1

Appendix E: Risk Predictive Model Monthly File..... E-1

Appendix F: Acronyms and Abbreviations ..... F-1

LIST OF FIGURES

Figure 1: Government Purchase Card Ecosystem..... 2

Figure 2: Card Request and Issue Data Flow..... 6

Figure 3: Purchase Card Use Data Flow ..... 8

Figure 4: Purchase Card Billing Data Flow ..... 14

Figure 5: Data Flow of Risk Predictive Model Data..... 16

Figure 6: Purchase Acceptance via WAWF Data Flow..... 18

Figure 7: Post Use Referral Data Flow ..... 22

Figure 8: PCOLS Reports..... 22

---

Figure 9: PCOLS Business Intelligence.....	22
Figure 10: DoD EMALL Process Flow .....	22
Figure 11: 3-in-1 Tool Data Flow .....	28

## LIST OF TABLES

Table 1. Parallel Data Flows of Purchase Card Usage Visibility and Oversight Data .....	11
Table 2. Purchase Card Billing Data Processing .....	12
Table 3. Processing of RPM Daily and Monthly Files .....	16
Table 4. Referral Notification Data from HNC .....	20
Table 5. Streamlined Approach .....	29
Table 6. Summary of Actions.....	29
Table B-1. One Transaction Detail Record per Transaction .....	B-1
Table B-2. One Account Detail Record per Unique Account .....	B-2
Table B-3. One Merchant Record per Unique Merchant.....	B-2
Table C-1. Bank Extract File Comparison to RPM.....	C-2
Table F-1. Acronyms and Abbreviations.....	F-1

## 1.0 OVERVIEW

This document describes the flow, transmission, and storage of Department of Defense (DoD) Micro-Purchase (MP) and Government-wide Commercial Purchase Card data. It provides a plan for optimizing data usage by streamlining data exchange and eliminating redundant or unused data and establishing data standards. This data management plan is a subset of an overarching Procurement Data Strategy under the governance of the Director of Defense Procurement and Acquisition Policy Defense Pricing/Program Development and Implementation (DPAP/PDI). This document is maintained by the Purchase Card Policy Office (PCPO).

Companion documents are:

Department of Defense Government Charge Card Guidebook for Establishing and Managing Purchase, Travel, and Fuel Card Programs. This document is referred to as the Charge Card Guide.

Government Purchase Card (GPC) Internal Controls Guide.

This is a living document. Version 1.1 was published in October 2010 and reflected the state of the program at that time. This second release of the plan is version 2.0. It is expected that the plan will continue to be updated on an annual basis to reflect the evolving DoD GPC and MP environment.

In addition to increasing GPC and MP data efficiency, this document is intended to provide a broad overview of the overall Purchase Card data “ecosystem”. This broad overview will enable stakeholders who work in one area of the “ecosystem” to have visibility into other parts of the “ecosystem”. See Figure 1 below for the major components and interconnections within the GPC Ecosystem. The end users of the document include people within the GPC Program authorization and usage hierarchy (cardholders, Approving/Billing Officials (A/BOs), supervisors, and Agency/Organization Program Coordinators (A/OPCs)) as well as support organizations (translation, routing, storage, analysis, and data mining).



The GSA SmartPay 2 program provides charge cards to U.S. government agencies through master contracts that are negotiated with major national banks. In June 2007, the Office of Charge Card Management awarded the ten year GSA SmartPay 2 master contracts to Citibank, JP Morgan Chase, and U.S. Bank. Through these contracts, agencies can obtain a number of different types of charge card products and services to support their mission needs. Qualified agencies issue a task order under the master contract.

The document is focused on the processing and data flows of the GPC SmartPay2 (SP2) providers, users, and data consumers. Although separate from SP2 with different requirements and processing approaches, the Air Force and Navy Non-Appropriated Funds (NAF) processing is addressed in the document where appropriate. Army NAF processing is part of SP2 and follows SP2 rules.

### **1.3 Document Vision**

The vision embraced by this document is that the Department will continue to mature its goal to implement data standards and processes across the GPC and MP functional areas. These data standards and processes will be incorporated into the DoD Business Enterprise Architecture (BEA). Maturation of the data standards and the BEA will allow the development of a Business Intelligence (BI) capability that will bring visibility of spend/demand data, track property accountability, and logistical allocations. This will result in enhanced support to the war fighter.

## 2.0 GOVERNMENT PURCHASE CARD DATA FLOW

### 2.1 GPC Account Request and Issue Process Overview

DoD has fielded an automated capability to manage the issuance and oversight of GPC Accounts in DoD. This electronic application is known collectively as the Purchase Card On-line System (PCOLS). The PCOLS suite of applications consists of five distinct components:

EMMA,  
AIM,  
PCOLS Reporting & Data Warehouse,  
Data Mining (DM), and  
Risk Assessment.

Each of these applications is a web-based application that uses the DoD Common Access Card (CAC) for authentication. The CAC Authentication is accomplished through the DMDC Single Sign-on (Sign-on and Referral System – SRS) functionality.

The Authorization, Issuance, and Maintenance (AIM) application is a workflow tool that draws from hierarchies recorded in the Enterprise Monitoring and Management of Accounts (EMMA) application. EMMA is a web application that allows users to be provisioned to use other applications. As part of the provisioning process, users can create and manage organizations and roles as well as assign users to the roles.<sup>1</sup> EMMA is used to authorize users in AIM, Data Mining, Risk Assessment, and the PCOLS Reporting modules within PCOLS. AIM, EMMA, and the PCOLS Reporting applications have been developed and are hosted and operated by the Defense Manpower Data Center (DMDC).

The Data Mining (DM) application and Risk Assessment (RA) application were developed by industry and currently are hosted by industry. In the 4<sup>th</sup> QTR FY2012 the DM/RA application hosting will be migrated to a DoD enclave. The PCPO established a contract in 2007 to perform Data Mining and Risk Assessment on DoD GPC Activity. The Data Mining / Risk Assessment (DM/RA) contract was awarded to HNC. HNC is generally the name referred to as the data mining provider that is a component organization of Fair Isaac Corporation (now called FICO). The DM application begins with a DoD specific rules-based component and a neural learning component that: (1) measures and reports the risk of all transactions no less than daily; (2) initiates requests for review of At-risk transactions no less than daily; (3) includes the user interface for transaction reviews; (4) creates and updates risk profiles for individual GPC Accounts based on buying patterns and review results no less than daily; and (5) stores and forwards the resolution results of At-risk transaction reviews.

Operational oversight of the program was initially being performed by DPAP/PDI/PCPO. Operational oversight for DM/RA will gradually migrate from the aforementioned office within

---

<sup>1</sup> “EMMA Application v. 4.3 User Manual”, EMMA Application v 4.3 User Manual – Document v1.3, August 2011.

the Office Secretary of Defense (OSD) to the Defense Logistics Agency (DLA). Currently, DLA maintains the PCOLS Help Desk and provides PCOLS training activities. DLA provides Level 1 and Level 2 Help Desk Support. DLA maintains PCOLS training material content and conducts webinar training and other classroom training. Defense Acquisition University (DAU) does provide online training and maintains PCOLS documentation that is available for download.

During FY2011, the planning process was accomplished to re-host the DM/RA applications within a DoD enclave. The rehost site will be the Defense Information Systems Agency (DISA) Defense Enterprise Computing Center (DECC) Mechanicsburg, located in Mechanicsburg, PA. Currently, the re-hosting is being targeted for completion by end of the calendar year 2012.

AIM functions as the gateway to the banks' systems. Together AIM and EMMA support a dual hierarchy, one that provides an audit trail for the acquisition/procurement authority, and one that provides an audit trail for the funding/command authority. The acquisition/procurement hierarchy for A/OPCs and the Resource Management (RM) hierarchy for Resource Managers are established in EMMA. The acquisition and funding hierarchies may be created interactively within EMMA or via a bulk load process. For the bulk load process to be used, the acquisition hierarchy must be provisioned down to the A/OPC Supervisor level and funding hierarchy must be provisioned down to the RM Supervisor level. The interactive process must be used to provision down to the A/OPC Supervisor and RM Supervisor levels. The acquisition hierarchy is populated with the roles and users down to the Cardholder's Supervisor level. The funding hierarchy is populated with all the roles and users down to the Resource Management Pool level. The roles and users from both hierarchies are assigned to account structures within AIM. A specific account is selected within AIM where managing and cardholder account requests are transmitted to the bank. Card issuance or maintenance requests are processed through AIM and transmitted to the bank for implementation. Some of this data (e.g., card status and card life-cycle information) will flow back to the DoD in the files that document account usage.

The hierarchy data is transmitted twice a day Monday-Friday by DMDC to the Data Mining/Risk Assessment third-party contractor for use in determining role based user access to the DM/RA application. This access allows for the review of GPC transactions and for the adjudication of At-risk transactions. Additional information such as account usage parameters and training records will be provided to the DM/RA application from AIM in the future.

The PCOLS Reports component of PCOLS Suite of Applications is intended to provide PCOLS Program Status Reporting and overall PCOLS Program Management Reporting. On the status reporting side, there are reports that cover account status, provisioning status, training due, etc. On the program status side there are reports that summarize the oversight of the program and the individuals responsible. Also, these reports summarize the data mining risk components and the adjudication of the At-risk transactions.

### **2.1.1 Request and Issue Data Flow**

Data is shared among the DMDC applications and transmitted to the bank and to the Data Mining application after appropriate approvals have been recorded. The hierarchy file is transmitted twice daily Monday-Friday to the Data Mining provider. Figure 2 illustrates the high-level data flow of initial and updated account, organizational, and hierarchy data.

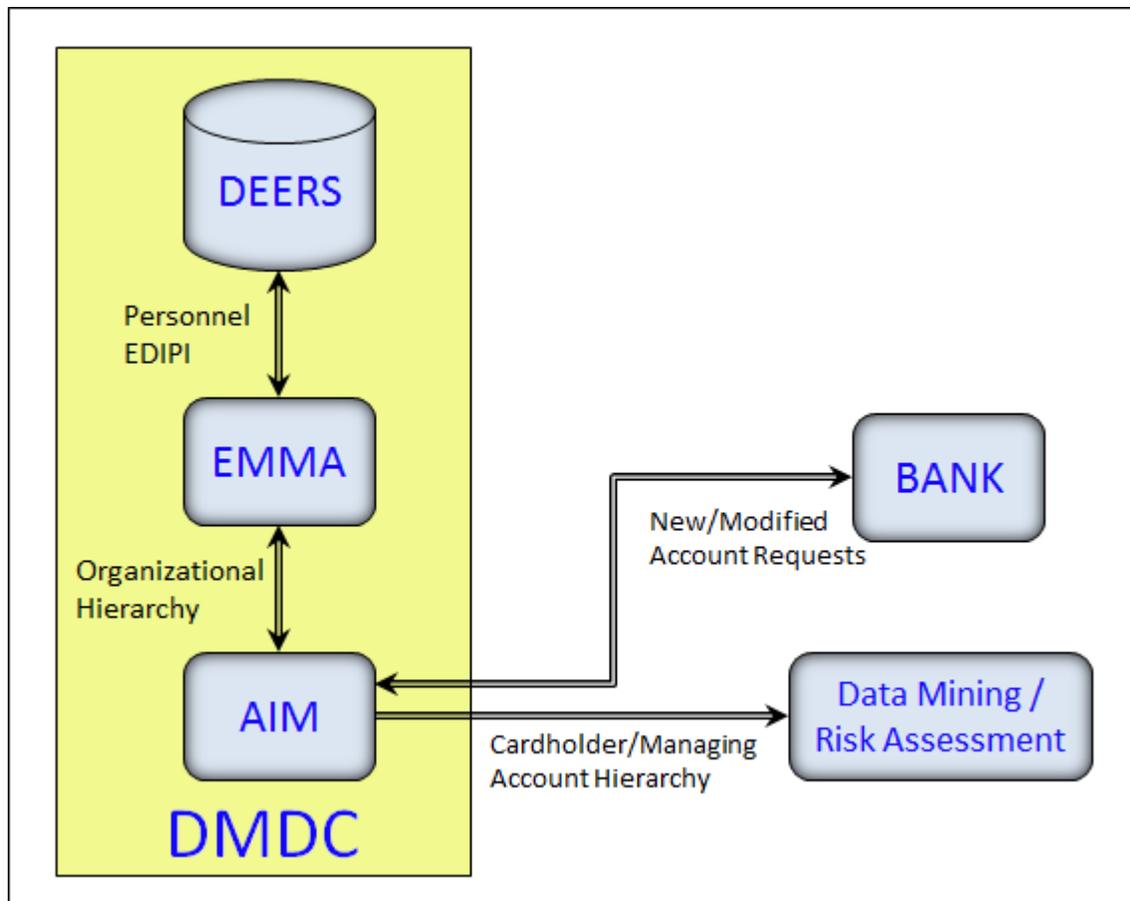


Figure 2: Card Request and Issue Data Flow

### 2.1.2 Request and Issue Data Capture and Retention

DMDC captures and tracks DoD personnel updates in DEERS, organizational relationships in EMMA, and manages workflow through AIM. The cardholder and managing account data is captured and retained within AIM. This data is forwarded to the banks and they confirm receipt and account status. In parallel, this organizational hierarchy data is sent to and stored by the DM/RA application for use in assessment of appropriate checks and balances of GPC Programs. The account hierarchy data that is provided to the Data Mining application is maintained in real time in the DMDC system; historical hierarchy information is not retained at DMDC, the banks, or the DM/RA provider. The PCOLS suite of applications retains current organizational state.

Account detail and hierarchy activation and maintenance can be performed in both the bank online system (Access Online for U.S. Bank and CitiDirect for Citibank) and through AIM. AIM receives data feeds from both banks to ensure that the bank data and AIM data are synchronized. According to the 19 November 2008 DoD Acquisition, Technology, and Logistics (AT&L) memo regarding PCOLS capability, the FOC goal is that no Purchase Cards will be issued except through the request generated by the AIM system. When fully implemented, this single process thread will enable increased oversight and traceability of account specifics and hierarchy.

While standard operating procedures should result in increased control by DoD systems and reduced reliance on bank systems, interaction directly with the bank systems should be available to support contingency or emergency situations where timing or lack of connectivity prevent standard process. As organizations deploy PCOLS, their ability to perform the same functionality directly through the bank should only occur on an exception basis, where PCOLS is not accessible and rapid response is required to meet contingency or humanitarian requirement. Functionality currently provided only by the banks, such as Line of Accounting modification and validation, is scheduled to be included in PCOLS in FY 2015. Once PCOLS is deployed to an organization, account setup and modification through the bank's direct input capability causes the potential for conflicting data to exist in the system. In addition to providing the Department with enhanced data, PCOLS provides greater control of the data. PCOLS is targeted to be the authoritative source of hierarchy data. Transitioning to PCOLS provides a gating opportunity to reconfirm the hierarchy and account detail currently established within the bank system. Changes made directly into the Bank's Electronic Automated System (EAS) are fed back to PCOLS to minimize conflict of data between PCOLS and the Bank's EAS. Once LOA maintenance capability is fielded in PCOLS, direct input of actions into the Bank's EAS will adversely impact the input of the data through the Bank's EAS.

## **2.2 Card Use Process Overview**

After GPC Account issuance and activation, a cardholder may use the Purchase Card for Government-authorized purchases only. Depending on mission needs, a cardholder may physically have a plastic card, or they may only have a 16 digit account number with appropriate validation/security codes for internet ordering or use as a payment vehicle on contracts. At the point of sale, data is captured regarding the sale and transmitted among fiduciary stakeholders.

### **2.2.1 GPC Account Use Data Flow**

Figure 3 illustrates the flow of transaction data during a purchase using the GPC Account. Data is transmitted, captured, and stored by each of these participants. The DoD's contractual and data visibility relationship is with the card issuing banks: U.S. Bank (Air Force, Army, and Defense Agencies), Citibank (Navy), and JPMorgan Chase (Air Force and Navy non-appropriated funds). Data retained by the credit card network (which includes processors such as Total Systems Service, Inc. (TSYS)) is available to DoD only via request to the card issuing bank.

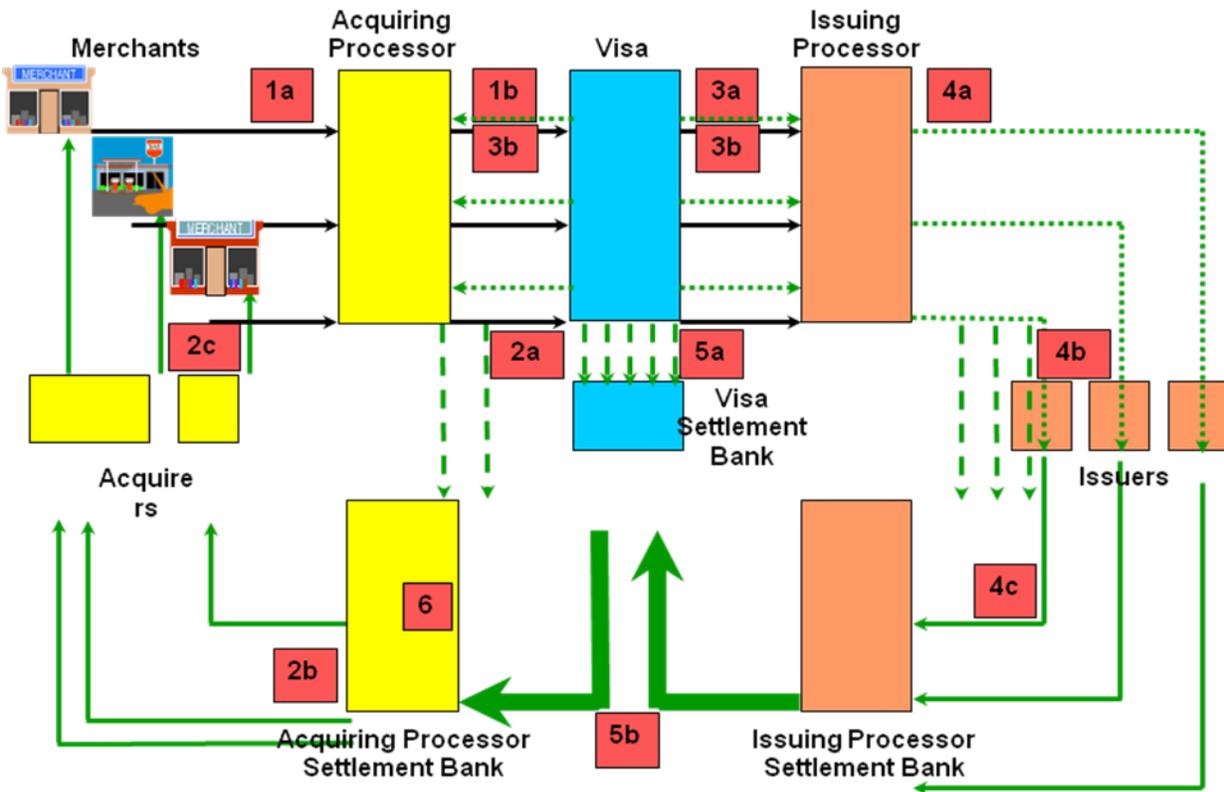


Figure 3: Purchase Card Use Data Flow

- 1a. Acquiring Processor collects Merchant transactions
- 1b. Processor forwards transactions to Visa
- 2a. Acquiring Processor passes instructions to its settlement bank for Merchant payment
- 2b. Processor's settlement bank initiates transfers from Processor's account to Merchant account at Acquirer
- 2c. Acquirer credits Merchant account for transactions
- 3a. Visa clears transactions to Issuing Processors
- 3b. Visa passes settlement information to Issuing Processors and Acquiring Processors
- 4a. Issuing Processor advises Issuers of their settlement positions
- 4b. Processor passes instructions to its settlement bank to debit Issuers and credit Processor's account
- 4c. Settlement bank transfers funds as requested
- 5a. Visa passes instructions to its settlement bank to:
  - Collect Funds from Issuing Processor settlement banks
  - Pay Funds to Acquiring Processor settlement banks
- 5b. Processor settlement banks transfer funds as requested
6. Acquiring Processor settlement bank uses Visa settlement to credit Processor account for payments to Merchants

In Figure 3, the Acquirer is also called the “merchant bank”. The issuing bank in the diagram is U.S. Bank, Citibank, or JPMorgan Chase depending on the service affiliation of the GPC Account holder.

## 2.2.2 GPC Account Use Data Capture and Retention

The DoD Contracted Banks provide GPC Account capability to DoD through Task Orders under the GSA SmartPay2 Master Contract that was awarded in June 2007. The transition from SmartPay1 to SmartPay2 occurred in November of 2008.

Note: JPMorgan Chase is not under a DoD SmartPay2 Task Order and, therefore, does not have the following requirements.

The SmartPay 2 contract requires the issuing bank to retain data as follows:

### Data Record Retention and Retrieval

In addition to the record retention requirements of Federal Acquisition Regulation (FAR) 4.703, the Contractor shall be the Government's agent for document repository as it relates to all transactions under the card program(s). The Contractor shall maintain electronic records of all transactions that exceed \$25,000 for a period of 6 years and 3 months after final payment, and for all transactions of less than \$25,000, for a period of 3 years after final payment. Final payment is defined as the final payment for the particular charge under each agency's/organization's task order. The Contractor shall segregate this transaction information (i.e., transactions exceeding \$25,000 and those less than \$25,000). Upon written request of the GSA Contracting Officer, the ordering Contracting Officer, the A/OPC, or the Internal Revenue Service with A/OPC knowledge and approval, the Contractor shall provide the requested information in an electronic format within 30 calendar days, unless otherwise specified at no additional cost to the Government. Also, Contractors/Banks shall provide online access to data for a minimum of 18 months after the transaction occurs.

Currently, it is not possible to identify from the GPC data those transactions less than \$25,000 that are applied as partial payments against contracts that exceed that threshold and require retention of the payment records for the longer 6-year and 3-month period. Similarly, a purchase exceeding \$25,000 may have multiple shipments; each resulting in a GPC payment transaction that individually does not exceed the threshold, but which needs to be retained for 6 years and 3 months to comply with regulation.

### Physical Record Retention

Cardholders and A/BOs have responsibility to capture and maintain GPC Account use records and receipts. Record retention requirements vary between cardholders and A/BOs. Generally for purchases at or below the micro-purchase threshold, retention of cardholder records is 3 years, if transaction(s) are above the micro-purchase threshold the retention period is 6 years and 3 months. The quick reference table of detailed requirements for retention of files in the FAR part 4.805 is below:

Document	Retention Period
(1) Records pertaining to Contract Disputes Act actions.	6 years and 3 months after final action or decision for files created prior to October 1, 1979. 1 year after final action or decision for files created on or after October 1, 1979.

(2) Contracts (and related records or documents, including successful proposals) exceeding the simplified acquisition threshold for other than construction.	6 years and 3 months after final payment.
(3) Contracts (and related records or documents, including successful proposals) at or below the simplified acquisition threshold for other than construction.	3 years after final payment.
(4) Construction contracts: (i) Above \$2,000	6 years and 3 months after final payment
(ii) \$2,000 or less	3 years after final payment.
(iii) Related records or documents, including successful proposals, except for contractor's payrolls (see (b)(4)(iv)).	Same as contract file.
(iv) Contractor's payrolls submitted in accordance with Department of Labor regulations, with related certifications, anti-kickback affidavits, and other related papers.	3 years after contract completion unless contract performance is the subject of an enforcement action on that date.
(5) Solicited and unsolicited unsuccessful offerors, quotations, bids, and proposals: (i) Relating to contracts above the simplified acquisition threshold.	If filed separately from contract file, until contract is completed. Otherwise, the same as related contract file.
(ii) Relating to contracts at or below the simplified acquisition threshold.	1 year after date of award or until final payment, whichever is later.
(6) Files for canceled solicitations.	5 years after cancellation.
(7) Other copies of procurement file records used by component elements of a contracting office for administrative purposes.	Upon termination or completion.
(8) Documents pertaining generally to the contractor as described at <a href="#">4.801(c)(3)</a> .	Until superseded or obsolete.
(9) Data submitted to the Federal Procurement Data System (FPDS). Electronic data file maintained by fiscal year, containing unclassified records of all procurements other than simplified acquisitions, and information required under <a href="#">4.603</a> .	5 years after submittal to FPDS.
(10) Investigations, cases pending or in litigation (including protests), or similar matters.	Until final clearance or settlement, or, if related to a document identified in (b)(1)-(9), for the retention period specified for the related document, whichever is later.

The general record retention requirement for A/BOs is 6 years and 3 months. However, if the transaction is funded by “foreign military sales funds,” retention is 10 years; if the transaction is in support of a contract payment, retention is 6 years and 3 months after final payment on the contract. Further guidance may be found in DoD Financial Management Regulation (FMR) Volume 5, Chapter 21 ¶2101.

Original disbursing office records (A/BO) along with cardholder supporting documents in electronic format (i.e., PDF format) negate the need to store duplicate hardcopy documents. Electronic record storage requires adequate controls to ensure that integrity of the digital images accurately represent the corresponding paper documentation and detect changes to an original digital image. In addition, electronic storage must be in a centrally managed location (i.e., not cardholder’s desktop) that has an established Continuity of Operations (COOP)/Backup process.

### Convenience Checks

When a convenience check is written for a payment for services (including any materials), rent, medical or health care services, or other IRS-required reporting services, the check payment event must be entered in the 1099 Tax Reporting Program (TRP) application operated by Defense Finance and Accounting Service (DFAS). Access to the 1099 TRP is requested through Form DD 2869. Data required by the 1099 TRP includes check number, check amount, date check is written, Tax Identification Number or Social Security Number (SSN), mailing address, and check recipient. Entry of this data by the check issuer into the 1099 TRP allows DFAS to accurately create and submit the IRS 1099 forms. Check events must be entered into the 1099 TRP no later than 31 December of the year the check is written. Note that this entry requirement does not apply to MP made with the GPC itself; the manual 1099 TRP entry requirement exists only when a service is acquired via a convenience check. The convenience check account holder is responsible to maintain audit trail of checks written to support 1099 reporting for 6 years and 3 months.

## 2.3 Usage Visibility and Oversight

Data related to the GPC ecosystem is provided to the Department from the banks each business day and at the conclusion of the monthly billing cycle. This data is transmitted in several formats to multiple recipients.

The following paragraphs describe the data received from the banks that is used by the DoD for processing, visibility, and oversight of GPC Account use. Table 1 identifies the data provided in parallel to DoD, the functional areas and uses supported, and the paragraph that further describes each data flow.

Table 1. Parallel Data Flows of Purchase Card Usage Visibility and Oversight Data

<i>Paragraph</i>	<i>Functional Use</i>	<i>Data Description</i>	<i>Periodicity</i>	<i>Data Recipient</i>
2.3.1	Purchase Card Billing Data	Obligations/Invoices	Daily/Monthly	Financial Systems
2.3.2	Data Mining / Risk Assessment Data	Custom Extract—Posting and Cycle Data	Daily/Monthly	Data Mining/Risk Assessment Provider

2.3.3	Wide Area Workflow Data	WAWF	Daily/Monthly	WAWF
2.3.4	Federal Procurement Data System Data	FPDS	Daily/Monthly	FPDS

### 2.3.1 Purchase Card Billing Data

Each weekday, data is transmitted from the issuing banks to the Department after processing by the transaction processing and authentication service providers such as TSYS. Similarly, after monthly billing cycle processing, invoice data is transmitted. The issuing banks, currently U.S. Bank and Citibank, expose the data on their systems. The DoD data routing and transformation hubs at either Defense Automated Addressing System Center (DAASC) or the DLA Global Exchange (GEX) pull the data and process it according to Table 2. The invoice (X12-810) and obligation (X12-821) data is based on the American National Institute of Standards (ANSI) X12 convention.

Table 2. Purchase Card Billing Data Processing

<i>Bank</i>	<i>Format</i>	<i>Hub</i>	<i>Translation</i>	<i>Recipient System</i>	<i>User Community</i>
Citibank	X12 821	DAASC	Yes	SABRS	Marine Corps
Citibank	X12 810	DAASC	Yes	CAPS-W	Marine Corps Entitlement
Citibank	X12 821; X12 810	DAASC	Yes	CABRILLO	SPAWAR
Citibank	X12 821; X12 810	DAASC	Yes	NERP	NAVAIR and NAVSUP
Citibank	X12 821; X12 810	DAASC	Yes	ILSMIS	Corona, Crane, Dahlgren, EODT, Indianhead, Port Hueneme, NUWC Newport
Citibank	X12 821; X12 810	DAASC	Yes	IMPS	Naval Research Lab
Citibank	X12 821; X12 810	DAASC	Yes	STARS	Navy
Citibank	X12 821; X12 810	DAASC	No	FASTDATA	Local Financial Management; SPAWAR
Citibank	X12 821; X12 810	DAASC	Yes	Maximo/DWAS	NAVFAC Information Technology Center (NITC)
Citibank	X12 810	DAASC	Yes	MSC	Receives both xlated file and raw X12
Citibank	X12 810	None	Yes; by Citi	SALTS	Supports afloat certification/tracking
U.S. Bank	X12 810	GEX	Yes	CAPS-W	Army
U.S. Bank	X12 810	GEX	Yes	CAPS-W	Agencies
U.S. Bank	X12 821	GEX	Yes	GAFS	Air Force
U.S. Bank	X12 821; X12 810	GEX	No	GFEBs	Army Financial ERP
U.S. Bank	X12 821; X12 810	GEX	Yes	IAPS	Air Force
U.S. Bank	X12 821	GEX	Yes	LMP	Army
U.S. Bank	X12 821	GEX	Yes	SOMARDS	Army
U.S. Bank	X12 821	GEX	Yes	STANFINS	Army
U.S. Bank	X12 821; X12 810	GEX	Yes	DBMS	Agencies
U.S. Bank	X12 821; X12 810	GEX	Yes	DAI	Agencies
U.S. Bank	X12 821; X12 810	GEX	Yes	EBS	Defense Logistics Agency

<i>Bank</i>	<i>Format</i>	<i>Hub</i>	<i>Translation</i>	<i>Recipient System</i>	<i>User Community</i>
U.S. Bank	X12 821; X12 810	GEX	Yes	DEAMS	Air Force
U.S. Bank	X12 821; X12 810	GEX	Yes	WAAS	Agencies

### **Purchase Card Billing Data – Data Flow**

In general, American National Standards Institute (ANSI) X.12 formatted Obligations (X12 821) are created daily and X.12 formatted Invoices (X12 810) are transmitted monthly by the banks. The DoD GEX and DAASC Hubs are configured to pull data from the bank sites periodically throughout the day. When data is present, it is processed and routed according to the internal Hub routing criteria to the appropriate accounting or entitlement system at the DFAS or Component financial systems. Routing is based on a combination of factors including file name and file content. Accountable Station and Obligation Processing Type Indicator (OPTI) are used to route Citibank files to Navy financial systems. As noted in Table 2, some recipient financial systems accept the X12 format and others receive a User Defined File (UDF) format after translation by the Hub.

Processing by the financial systems establishes the obligations in the accounting systems and posts the monthly invoice to the entitlement systems. Based on internal processing rules, DFAS (or the disbursing system) pays the bank for the charges incurred by the cardholder. Rebates are calculated based on the net purchase volume and the latency between the date of purchase and the posting of payment.

The invoice files reflect charges incurred by the cardholder and approved by the Approving/Billing Official (A/BO) in the bank's online system. In the case of Navy afloat situations, Citibank creates a spreadsheet of posted cardholder transactions that is transmitted through DAASC to the Standard Automated Logistics Tool Set (SALTS). Approving/Billing Officials (A/BOs) download the spreadsheet from SALTS, certify transactions, and transmit the certified transactions through SALTS back to Citibank. Citibank then creates invoices that reflect the SALTS-certified transactions. This approach enables afloat units or those operating in low communication environments to interact with the Citibank Purchase Card system. The OPTI code of "S" indicates transactions that are routed to and certified through the SALTS process.

The non-appropriated funds Purchase Card billing process does not follow the general flow described above. For purchases made with this type of card, a direct connection is established between the Air Force and the JPMorgan Chase system. Each day, transactions that were certified on the PaymentNet online system 4 days prior are pulled. The transaction data is processed and paid the following day. This approach enables these types of accounts to maximize rebate amount.

Figure 4 illustrates the data flow from the banks to DFAS for obligation and invoice data.

## Purchase Card Billing Data Flow

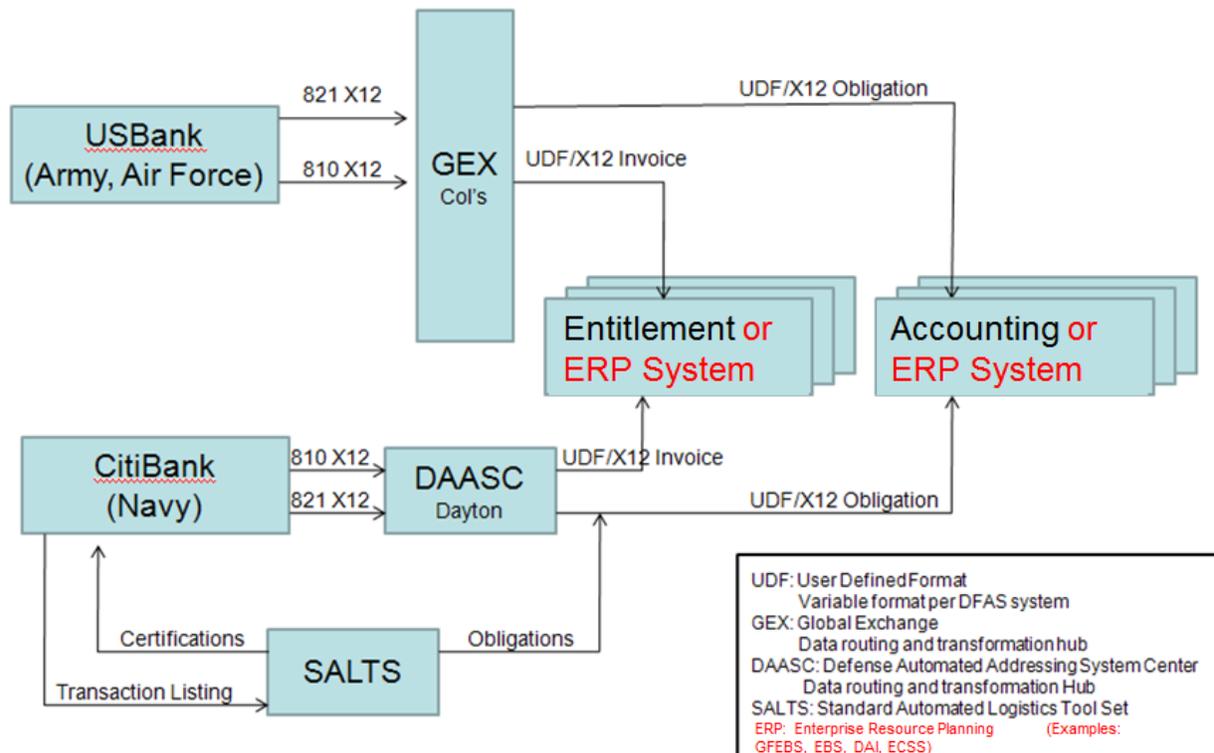


Figure 4: Purchase Card Billing Data – Data Flow

### GPC Account Billing Data – Use and Retention

The GPC Account billing data is used to establish obligations and set the entitlement for payment of the GPC invoices. It is expected that the obligation and invoice data provided by the banks supports disbursement and is therefore retained by DFAS for at least a 6 year and 3 month period in compliance with the DoD Financial Management Regulation Volume 5, Chapter 21; however, confirmation with each financial system was not attempted. The data is retained in the DAASC and GEX online archives for approximately 6 months and is then moved to offline storage. Access to offline storage is possible, but is costly and time consuming.

#### 2.3.2 Data Mining / Risk Assessment Data

Fraud detection is critical to efficient execution of the DoD GPC Program as detailed in the March 2008 Government Accountability Office (GAO) Report “Actions Needed to Strengthen Internal Controls to Reduce Fraudulent, Improper, and Abusive Purchases.” In parallel, the Navy performs fraud detection using a third-party vendor that executes the Program Audit Tool (PAT). The PAT receives data in the Citibank Commercial File (CCF) format. Transactions are flagged for review based on business rules. The PAT tool uses the hierarchy within the CCF file

to address email notifications. These notifications are used to facilitate the review and dispositioning of flagged transactions. Also, there is an escalation process.

As mentioned in Section 2.1 – GPC Account Request and Issue Process Overview, DoD has implemented PCOLS for GPC Program oversight. The Navy started a PCOLS Pilot Program in March 2010 for both CONUS and OCONUS sites. The PCOLS Pilot Deployment enabled a comprehensive and conclusive assessment of its capabilities. At the conclusion of the pilot deployment, DON found that a Navy-wide deployment of PCOLS would have significantly diminished DON GPC Program oversight and reporting capabilities. After the conclusion of the pilot, the DON indicated that they remain committed to the PCOLS concept. Once identified improvements to PCOLS have been completed, the DON indicated that they will conduct a Business Case Analysis to determine if adopting PCOLS is in the best interest of the Navy.

The primary function of data mining is to detect fraud, waste, abuse, and misuse. The current DM/RA functionality is different from previous misuse analysis capabilities because it has a learning component that discerns acceptable usage behavior over time and, therefore, attempts to minimize “false positive” findings that distract program officials from true misuse findings.

The DM/RA contractor defined file formats that contain data specific to their mission. A bank-agnostic, common daily transaction file and monthly cycle file have been defined. These files are called the Risk Predictive Model (RPM) files. U.S. Bank and Citibank each create the RPM format and expose it for retrieval by the DoD data transformation and routing Hubs. JPMorgan Chase is not currently generating the RPM files. JPMorgan Chase services non-appropriated funds and does not hold a Smart Pay 2 contract Task Order for DoD. The intent is to acquire RPM data from JPMorgan Chase at a later time. Business rules specific to non-appropriated funds will be applied at HNC/FICO once the data is provided by JPMorgan Chase. Requirements definition for AF-NAF is expected to start in FY 2015

The daily RPM files received from U.S. Bank have a latency of two (2) days. In order to provide the Merchant Identification element, U.S. Bank holds the daily transactional data for 2 days before transmitting it to DoD. The DoD and U.S. Bank have established an initiative to update the U.S. Bank process to eliminate the 2 day latency data issue. This initiative should be accomplished in FY 2012. Citibank data does not experience this latency.

No data transformation is performed on the RPM files. The data is routed directly to DMDC without modification. Once the data arrives at DMDC, the files are passed without modification to HNC/FICO.

DMDC provides value by monitoring the receipt of the file by setting a cron job that checks for the file every hour for 5 hours after it is expected (U.S. Bank 7am CT; Citibank 1pm CT, Tues–Sat). If the file is not received, email alerts are generated and escalation process initiated to identify and resolve issues.

The files are transmitted to HNC/FICO and then a trigger file is placed at HNC/FICO to let them know that the file has been completely transmitted (to avoid HNC/FICO file retrieval during transmission by DMDC).

### Data Mining / Risk Assessment Data – Data Flow

The RPM files are not used by DMDC. The daily and monthly RPM files are currently stored intact. Appendix D contains the file structure defined by HNC/FICO for the RPM data Daily files. Appendix E contains the file structure defined by HNC/FICO for the RPM data Monthly files.

Figure 5 illustrates the current data flow of the RPM files for both daily and monthly files.

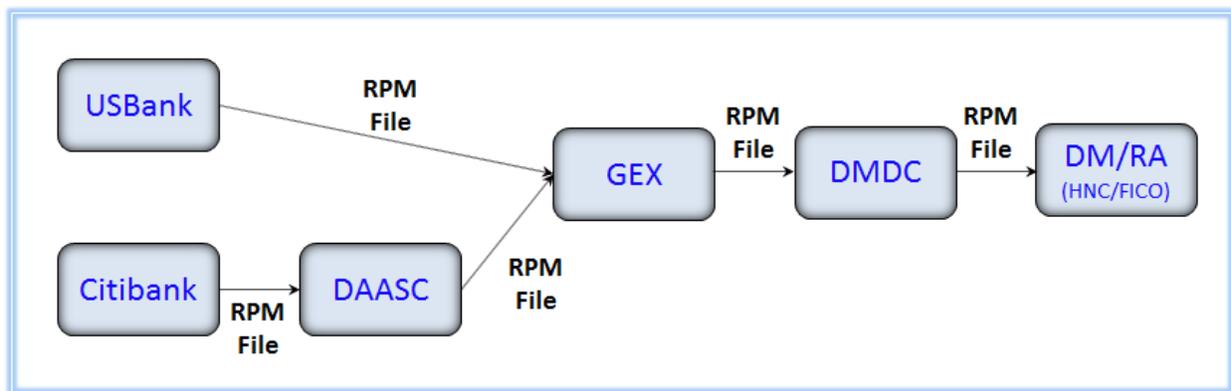


Figure 5: Data Flow of Risk Predictive Model Data

Table 3 identifies the file names of the data files that are transmitted from the banks through the DoD infrastructure to HNC/FICO.

Table 3. Processing of RPM Daily and Monthly Files

Bank	Format	Inbound from Bank to GEX file name	Map	Outbound from GEX to DMDC and from DMDC to HNC file name	Comment
U.S. Bank to GEX to DMDC	DOD_RPM_Layout_v1.2_External.200 81013.xls	P200.P20DHNCD.X320	None	US_HNC_Dailyfileymmddhhmmss	Daily
	DOD PCARD Account Cycle Data Layout v1 13_FINAL.xls	P200.P20DHNCD.X320	None	US_HNC_accountcycleymmddhhmmss	Monthly
Citibank to DAASC to GEX to DMDC	DOD_RPM_Layout_v1.2_External.200 81013.xls	CITI-DOD-RPM*	None	CITI-HNC-CITI-DOD-RPM-DAILY	Daily
	DOD PCARD Account Cycle Data Layout v1 13_FINAL.xls		None		Monthly

### Data Mining / Risk Assessment Data – Use and Retention

Daily and monthly data are provided by the banks to support the Data Mining initiative. The monthly Reconciliation data contains a subset of the daily RPM data elements that are transmitted daily. The reconciliation file received by DMDC monthly is dissimilar in nature to the DM/RA monthly cycle data. Appendix C defines the data elements provided by each bank for Account, Transaction, and Merchant data. For each element provided in the Bank Extract data, the related RPM Daily File element is identified. (JPMorgan data elements are prospective based on design documents; this data is not yet in production). Appendix C illustrates that there are some differences in the data provided by the banks. The common DM/RA data format

provided by all the banks includes 92% of Transaction data, 76% of the Account data, and 23% of the Merchant data provided by the banks in the reconciliation files. Much of this data between transaction, account, and merchant files is redundant and the government chose not to have it repeated. Additionally, for PII purposes, the government determined that cardholder name and phone number should not be included.

The RPM files destined for HNC/FICO are stored at DMDC as-is (not parsed into a database). The retention period will be determined by a Memorandum of Understanding (MOU) between DMDC and the PCPO that has not yet been established.

### **2.3.3 Wide Area Workflow Data**

The Government Accountability Office has stated that accountable property acquired or paid for with the GPC needs to be recorded in property systems and must have independent receipt and acceptance. Wide Area Workflow (WAWF) has been enhanced to support this functionality.

#### **WAWF Government Purchase Card Receiving Report**

The initial implementation of WAWF accommodates the situation when goods are acquired through a contract vehicle where the GPC is used as the method of payment. When those conditions exist, the vendor will submit an Advance Shipment Notification (also called the DD Form 250 or Material Inspection and Receiving Report) via WAWF at the time of shipment. In addition to the standard data elements, four GPC specific elements are captured. The vendor can submit the data electronically or input the data via the WAWF web input screens. When acceptance occurs, WAWF will send an electronic notification to the property book system to record receipt of the property.

After Government acceptance of the property in WAWF, the data will flow to the DMDC based on the "Pay DoDAAC" of "CRCARD." Entry of this Pay DoDAAC will prevent the data from entering the payment process and will ensure that the data is transmitted to DMDC. DMDC will capture and store the data. In the future, the data received from WAWF will be compared to the GPC transaction data transmitted by the banks to identify potential misuse. The accountable property purchased using the GPC and accepted in WAWF can be transmitted to property accountability systems of record based on routing criteria established at the GEX, or provided by the designated government accepting official.

#### **Purchase Acceptance via WAWF Data Flow**

Figure 6 illustrates the data flow for acceptance data related to property acquired via contract using the GPC. When the GPC is used as method of payment for goods acquired via a contract, the vendor submits the data to WAWF, and the Government acceptor performs the acceptance action in WAWF. Also, the diagram illustrates that the acceptance may be performed externally to WAWF, but the vendor interaction and post-acceptance data flow will be via the WAWF application.

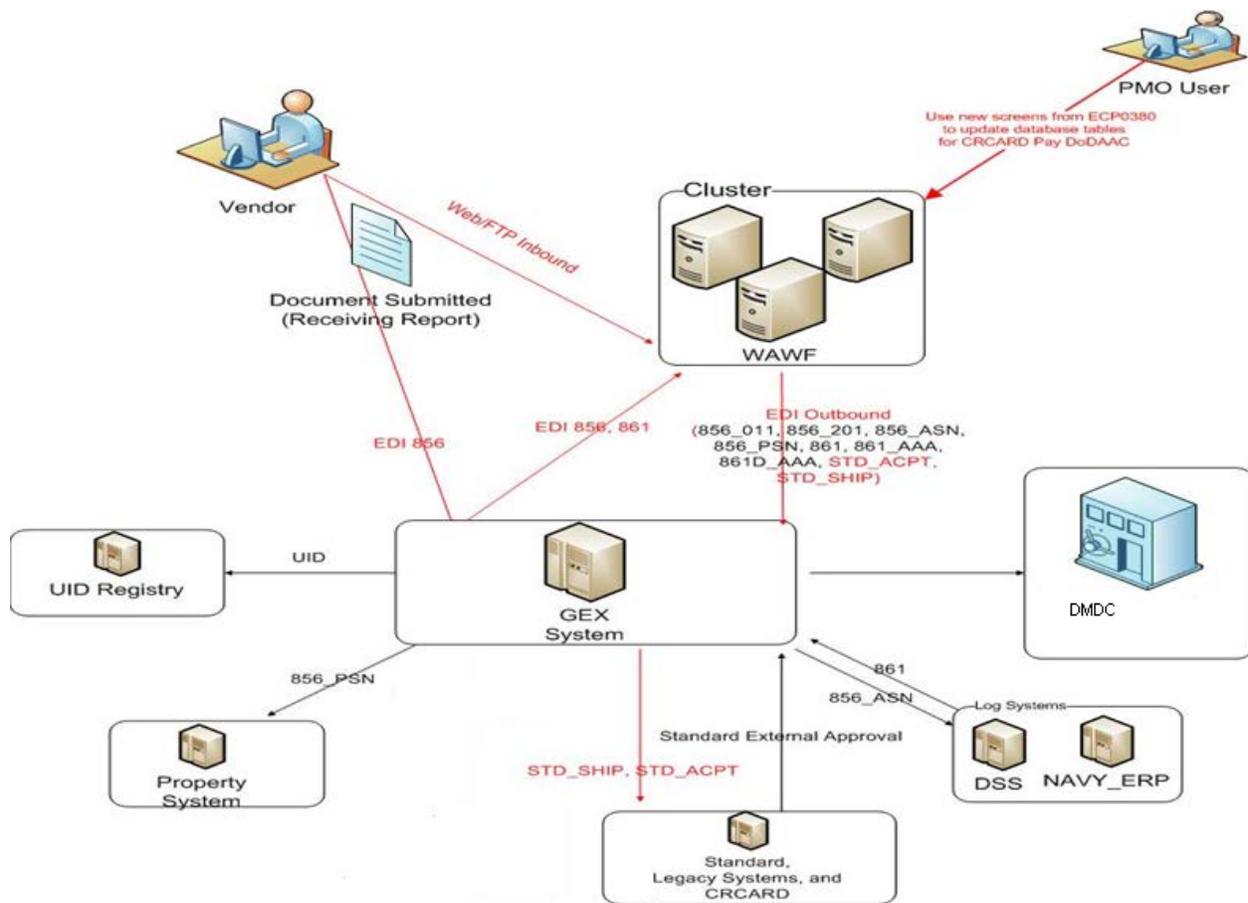


Figure 6: Purchase Acceptance via WAWF Data Flow

After Government acceptance of the goods, the acceptance data including the GPC specific elements will flow to DMDC. The data elements entered by the vendor when submitting data about goods acquired by a contract where the GPC is the payment vehicle are: Vendor Identifier, Vendor Transaction Number, Issuing Bank, and Amount Billed. Based on the vendor entry of the “Pay DoDAAC” of “CRCARD”, the data will flow to DMDC.

### Purchase Acceptance via WAWF – Use and Retention

The WAWF Standard transaction, including the GPC specific data elements, will be transmitted to DMDC. The GPC specific data elements will enable association of the acceptance data entered in WAWF with the GPC transaction data received from the banks. Conditions or attributes of the relationship between these data sources will identify purchases that may require review.

The acceptance data will be processed by WAWF and retained by DMDC. It is expected that DMDC will use a retention period of 6 years and 3 months for acceptance of goods acquired via a contract where GPC was the payment vehicle.

### **2.3.4 Federal Procurement Data System Data**

The Federal Procurement Data System (FPDS) provides a comprehensive web-based tool for agencies to report contract actions. The resulting data provides the following:

- 1) A basis for recurring and special reports to the President, the Congress, the Government Accountability Office, Federal executive agencies, and the general public;
- 2) A means of measuring and assessing the effect of Federal contracting on the Nation's economy and the extent to which small, veteran-owned small, service-disabled veteran-owned small, HUBZone small, small disadvantaged, women-owned small business concerns, and AbilityOne nonprofit agencies operating under the Javits-Wagner-O'Day Act, are sharing in Federal contracts; and
- 3) A means of measuring and assessing the effect of other policy and management initiatives (e.g., performance based acquisitions and competition).

FPDS does not provide reports for certain acquisition information used in the award of a contract action (e.g., subcontracting data, funding data, or accounting data).

Executive agencies use FPDS to maintain publicly available information about all contract actions exceeding the micro-purchase threshold, and any modifications to those actions that change previously reported contract action report data, regardless of dollar value. Agencies awarding assisted acquisitions or direct acquisitions must report these actions and identify the Funding Agency Code.

All awards, regardless of dollar value, in the Small Business Competitiveness Demonstration Program (Comp Demo) designated industry groups (i.e., Construction, A-E, Trash & Refuse, etc.) (FAR 4.606(a)(2)).

### **Federal Procurement Data System Retention**

Federal Procurement Data System stores all data associated with the application indefinitely.

## **2.4 Post Use Review**

Data Mining and Risk Assessment of GPC transactions and management organizations are provided by HNC/FICO, which has expertise in neural networks and data mining capability. The Data Mining/Risk Assessment contractor merges the daily and monthly Risk Predictive Model data provided by the banks with the user/account hierarchy data provided by DMDC PCOLS/AIM. This process is described in Section 2.3.2 of this document. The GPC Account use activity contained in the data provided by U.S. Bank and Citibank (see Figure 5) and the hierarchy of users provided by DMDC (see Figure 2) is evaluated against the Data Mining Risk Predictive Models.

Appendix D defines the aggregation of the daily RPM data format required by the DM/RA application from the banks and the data anticipated from PCOLS related to accounts and account holders. HNC/FICO receives the bank data and the PCOLS data separately and subsequently aggregates it.

Once the RPM data file has been evaluated against the risk predictive model, a score is assigned to the transaction. The score assigned to the transaction determines if the transaction is considered At-risk of fraud, waste, abuse, or misuse. These At-risk transactions require human evaluation by the responsible A/BO. Transactions that score exceptionally high are referred to as high-risk transactions and require an Independent Review (IR) by the A/OPC. This IR is in addition to the A/BO review.

The Daily Scored Transaction File contains all of the GPC transactions with the score assigned by the risk predictive model. This file is transmitted daily from Data Mining to DMDC (see Figure 7 #1).

An At-risk transaction file is transmitted daily from Data Mining to DMDC (see Figure 7 #2) identifying the At-risk transactions and current status of the review process. Table 4 lists the referral file data received by DMDC. Based on this data, an email is transmitted to the appropriate recipient in the chain of command based on the account hierarchy retained in PCOLS and related business rules. The email contains information about the At-risk transaction including the account, merchant, and date of the transaction. A link to PCOLS that is used to access the HNC/FICO case management tool is also included in the email. The email recipient uses the link to log into PCOLS to access the DM Case Management tool and to track and input the resolution of the At-risk transaction through that tool. There is an escalation process associated with the dispositioning of At-risk transactions. If action is not taken on a case within predefined time periods, the email notifications will escalate up through the hierarchy.

HNC/FICO transmits to DMDC daily the Daily Archive File (Case History) (see Figure 7 #5). This file contains any and all modifications to a referred transaction (i.e., updates to the transaction during the case dispositioning process).

Table 4. Referral Notification Data from HNC

<i>Data Element</i>	<i>Data Definition</i>
caseNumber	Case Number for the Cardholder Account
transactionId	Unique ID to identify transaction
caseStatus	Status of Transaction—Following Values: <ul style="list-style-type: none"> <li>• 0 – New Case</li> <li>• 1 – Under A/BO Review (Pending)</li> <li>• 2 – Closed</li> </ul>
Edipi	User EDIPI who last acted on the case
caAccountNumber	Cardholder Account Number
maAccountNumber	Managing Account Number
caseDisposition	Must be one of the following: <ul style="list-style-type: none"> <li>• V – Valid Transaction</li> <li>• A – Administrative Discrepancy</li> <li>• M – Misuse</li> </ul>

	<ul style="list-style-type: none"> <li>• S – Suspected Fraud</li> <li>• B – Abuse</li> <li>• L – Lost</li> <li>• T – Stolen</li> </ul>
notificationType	Must be one of the following: <ul style="list-style-type: none"> <li>• T – Flagged Transactions</li> <li>• Q – Quarterly Report Completion</li> </ul>
transDateTime	Transaction Date Timestamp
tranAmount	Transaction Amount
merchantName	Merchant Name
mccCode	Merchant Category Code
firstTransmissionDate	First Transmission Date
Score	Score assigned to case by Data Mining Risk Predictive Model

Monthly files are also provided by U.S. Bank and Citibank to Data Mining via DMDC. The structure of the monthly file is included as Appendix E. There is no monthly data transmission from PCOLS to Data Mining.

### Post Use Data Flow

The DM/RA data flow and numerical sequence are illustrated in Figure 7. All DoD GPC transactions feed into Data Mining and all relevant transactions are scored by HNC/FICO Risk Predictive Model. This scored transactions file is sent to DMDC for subsequent storage and use (Figure 7 #1). At-risk transactions (flagged transactions) generate new cases by the Data Mining application. These cases are based on the assigned score from the risk predictive model and also random transactions used to baseline the model. Data for email notifications are sent to the DMDC in At-risk File (Referral File) (Figure 7 #2). The DMDC identifies the email address for the recipients of referral notifications and transmits the email messages (Figure 7 #3). Emails are sent for New Cases, Closed Cases, and Escalated Cases. DoD Personnel perform the analysis, documentation, and dispositioning of the case using DM Case Manager (Figure 7 #4). Case history is transferred to DMDC (Figure 7 #5). This case history is used by the PCOLS Reporting application (see Figure 9).

To obtain access to the DM Case Manager, DoD Personnel are authenticated by their Common Access Card (CAC) through the Sign-on and Referral System (DMDC Single Sign-on (SRS)). Once authenticated, the user's credentials are passed from DMDC to DM/RA. DM/RA then grants role based access to the Case Manager for these CAC credentialed personnel.

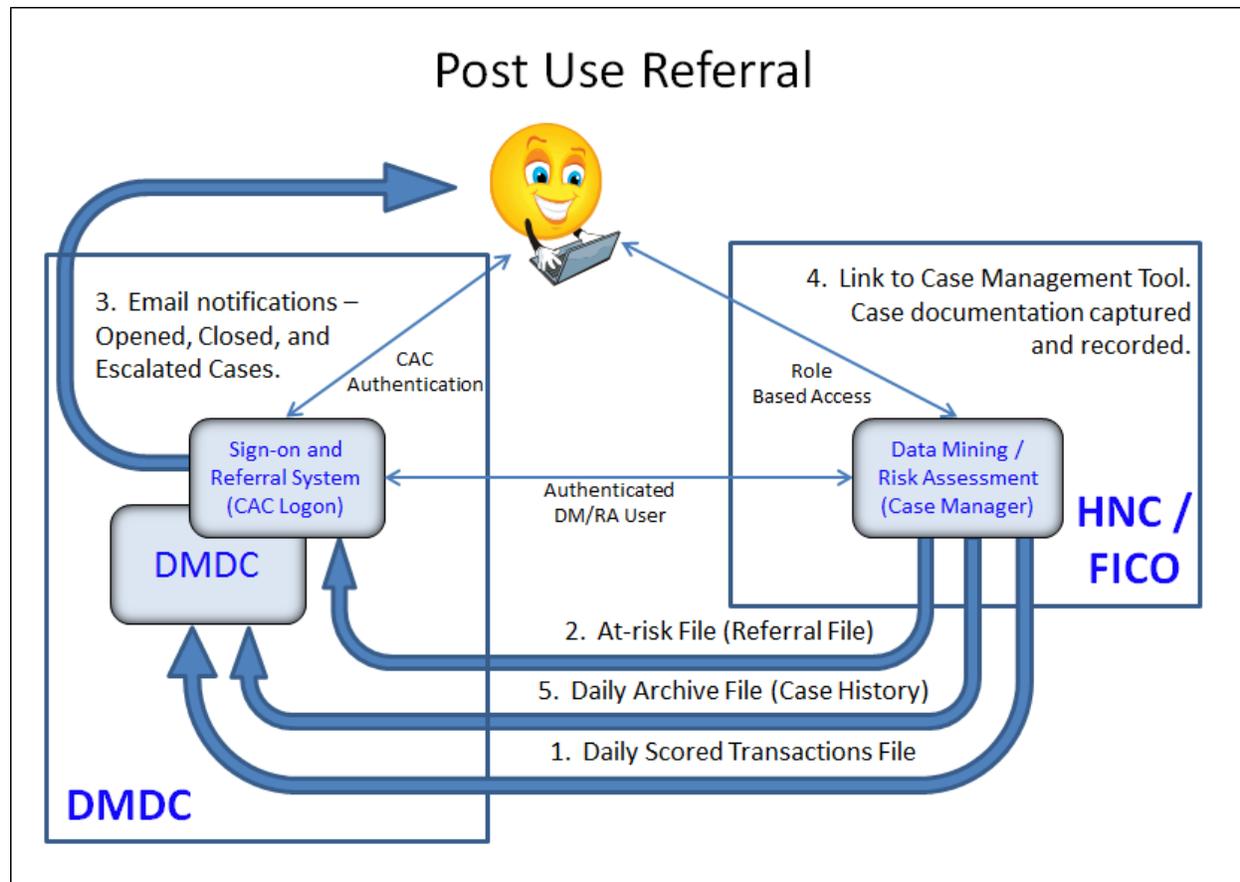


Figure 7: Post Use Referral Data Flow

## Post Use Data Retention

The account hierarchy data is maintained in real time at DMDC; the hierarchy as it existed on a given day is not retained. DMDC stores the Daily Scored Transactions file intact indefinitely. DMDC stores the Daily Archive file (Case History) intact indefinitely. The retention period for the Daily Scored Transaction file and the Daily Archive file will be defined in the MOU between DMDC and the PCPO.

Because the DM/RA contract is a services contract, specific data retention requirements are not defined. GPC data is retained in two environments by two vendors at data center facilities. The data is received, processed, and archived on a production server. The data used to enhance the risk predictive model is captured and processed in the modeling server environment. The DM/RA applications report on a rolling 18 months of data. Older data is archived off the production servers.

## 2.5 Business Intelligence

The data stored in the DM/RA and PCOLS applications needs to be accessible so that it exhibits the tenets of net-centric acquisition, which are:

- **Common, clean, consistent data**
- **One version of the truth**
- **Across the entire Department of Defense**
- **Accessible at any authorized level**

It is the stated goal of the PCOLS Data Strategy that Business Intelligence will be infused into the data standards and PCOLS architecture so that it meets the tenets of net-centric acquisition in order to meet reporting and decision support needs as it grows to full DoD wide implementation.

## 2.6 PCOLS Business Intelligence

Currently, the PCPO is working closely with DMDC to provide a Business Intelligence (BI) solution with the data feed from DM/RA. The PCOLS Data Warehouse was developed and initial population occurred in November 2011. At that time, the first report was made available in production. This report was the Program Management Report. This report contains consolidated information for the management of DoD GPC Program. The information contained on this report is broken into five major categories:

1. Program Summary (number of transactions, number of flagged transactions (DM/RA At-risk transactions), etc.)
2. Monthly Account Review (number of A/OPCs, A/BOs, Cardholders and other relevant account information)
3. Report Card – Program Health (key controls based on current RA application),
4. Case Disposition (DM/RA at risk transaction adjudication summary), and
5. Infraction Category (infractions reported from DM/RA).

Additional reports were deployed in FY 2012. These reports are:

Case Disposition Summary Report,  
Case Disposition Detail Report,  
Recommended Action Summary Report, and  
Infraction Detail Report.

These reports generally are based on the decomposition of the Program Management Report. The PCOLS Reporting functionality continues to be built out. Additional reports are in analysis and development and these reports will soon be available to the PCOLS user community. See Figure 8 below for a list of all current PCOLS Reports.

Summary	Description
1. Purchase Card Report	Report lists all ACTIVE Cardholder Accounts that meet the criteria requested (organization, card or convenience check, special designation). Report includes cardholder name and contact information, card/check indicator, special designations (if any), warrant amount (if applicable), and purchase limits.
2. Conflict of Interest Report	Report includes individuals that are a Primary/Alternate A/BO and a Cardholder within the same managing account. Report is run at the A/OPC organization level and includes conflicts for all subordinate managing accounts.
3. A/BO Report	Report identifies the Primary and Alternate A/BOs and associated managing account. Report will identify associated organization or sub-organization name.
4. Workflow Aging Report	Report includes account requests that have been in workflow over a specified length of time. Requests will include new managing and cardholder accounts as well as maintenance requests.
5. Provisioning Status Report	Report identifies all users provisioned under a selected organization and provides the provisioning status of active or pending. Report identifies associated organization or sub-organization name and includes user's name, email address, and role.
6. Training Due Report	Report includes Primary A/BOs and Cardholders with training requirements due within the requested time period. Includes supervisor contact information.
7. Annual Review of Managing Accounts Report	Report includes all ACTIVE Managing Accounts that require the annual review within the requested time period. The Annual Review due date is entered by the A/OPC on each account.
8. Account Status Report	Report includes account totals per status at A/OPC organization level
9. Program Management Report	Report provides summary organization information on transactions and DM/RA cases. Report can be generated for any organization A/OPC or above. Report can only be run for 1 bank cycle.
10. Case Disposition Detail Report	Report provides details of case dispositions by A/OPC organization. Report only includes cases that were given a disposition of Abuse, Misuse, Suspected Fraud, Lost, Stolen, or Administrative Discrepancy. Report can be generated for any organization A/OPC or above, but always lists A/OPC orgs. Report can only be run for 1 bank cycle.
11. Case Disposition Summary report	Report provides summary of case dispositions by A/OPC organization. Report can be generated for any organization A/OPC or above, but always lists A/OPC orgs. Report can only be run for 1 bank cycle.
12. Recommended Action Report	Report provides summary of case dispositions and planned actions. The counts should be a total for the organization selected on the report criteria page.
13. Infraction Detail Report	Report provides details of infractions by A/OPC organization. Report includes all infractions from cases with a disposition and a transaction date within the report criteria. Report can be generated for any organization A/OPC or above, but always lists A/OPC orgs. Report can only be run for 1 bank cycle.

Figure 8: PCOLS Reports

PCPO does expect that PCOLS Reporting will subsume all of the RA functionality in the near future. RA will include the dashboard reporting and the quarterly reports. PCPO is working with DMDC to expand the reporting capabilities of the PCOLS Reporting & Data Warehouse. The IBM Cognos BI capability is being used by DMDC for the PCOLS BI.

The figure below describes the data flow from DM/RA into the PCOLS Reporting & Data Warehouse. Access to this data is through PCOLS Reporting. Note that the SRS functionality is used for CAC authentication.

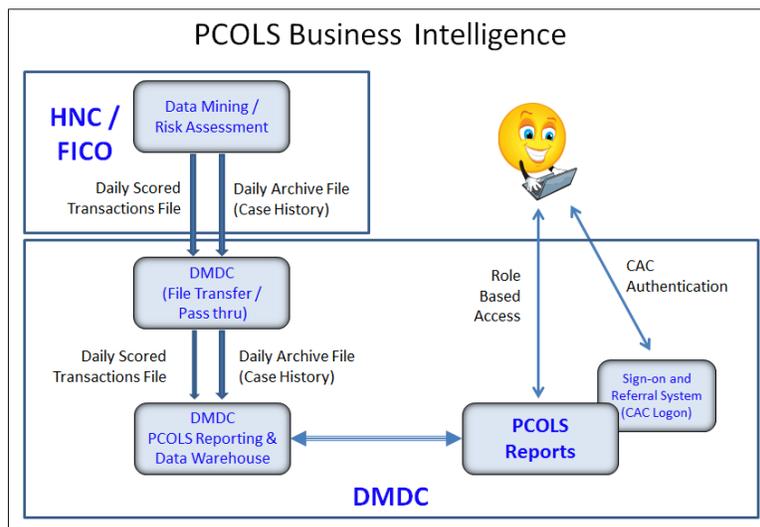


Figure 9: PCOLS Business Intelligence

## **2.7 Office of Management and Budget (OMB) Reporting**

Currently, the PCPO is provided consolidated data from the banks and the components to meet the reporting requirements of OMB Circular A123. Once consolidated, this data is posted on the OMB reporting web site. Also, the banks are providing an electronic data feed to the General Services Administration (GSA) for the posting of additional detail at USAspending.GOV. The posting of the data at USAspending.GOV is in three phases with each phase providing more granular detail. Currently, we are in Phase 1, which posts the data at senior service level with all defense agencies combined. When version 2.1 of USAspending.GOV is fielded, data will be aggregated by 30 merchant category codes (MCC). All posted DoD data is on a 90 day delay for operational concerns. In Phase II, it has been requested that data contain all MCC codes, be at Sub-agency level, and contain ZIP+4 code (Congressional district). DoD policy is to not post data at Sub-agency level as that would expose operationally sensitive data even with the 90 day delay. In the current process, the rolled up value of all transactions are posted. Until the process limits data to approved/certified transactions, DoD objects to posting data below the MCC cluster level. DoD has not agreed to posting at the Congressional district level because the logic to determine district has not yet been developed. In Phase III, it is the goal to post all transactions. Implementation dates for the phases have not been identified. DPAP/PDI/PCPO will continue to coordinate with GSA on the appropriate posting of GPC data.

### 3.0 DATA, PROCESS STANDARDIZATION, AND SECURITY

The credit card industry has developed data processes and system standards to minimize risk of fraud and prevent identity theft. The DoD fully supports these efforts. Therefore, all changes to the operating system environment should be approved and documented in accordance with the DoD Information Assurance Certification and Accreditation Process (DIACAP) process. This will ensure system and data integrity. The DIACAP is used to govern system administration for all DoD systems supporting the GPC Program. The Bank’s EAS will comply with the Payment Card Industry (PCI) Data Security Standard (DSS). Transmission of all electronic account data is processed through secure lines of communication. During FY 2012 the DoD needs to work with the card associations and the banks to ensure that all system issues associated with PCI standards and DIACAP are appropriately mitigated.

#### 3.1 DoD EMALL

The DoD EMALL operates as a vendor, and, therefore, must be PCI compliant. The acquiring bank for EMALL is Fifth Third Bank. The DoD is in the process of codifying policy that all “malls” must require their vendors to provide Level III enhanced GPC transaction data on all GPC transactions. All orders placed on a “mall” are contract actions that are subject to Federal Procurement Data System (FPDS) reporting requirements. In addition to Level III enhanced data and FPDS reporting requirements, the “malls” are required to provide a feed that will populate the Banks EAS along with WAWF/EDA for all orders placed. For the DoD EMALL, a detailed process flow may be found below (Figure 10).

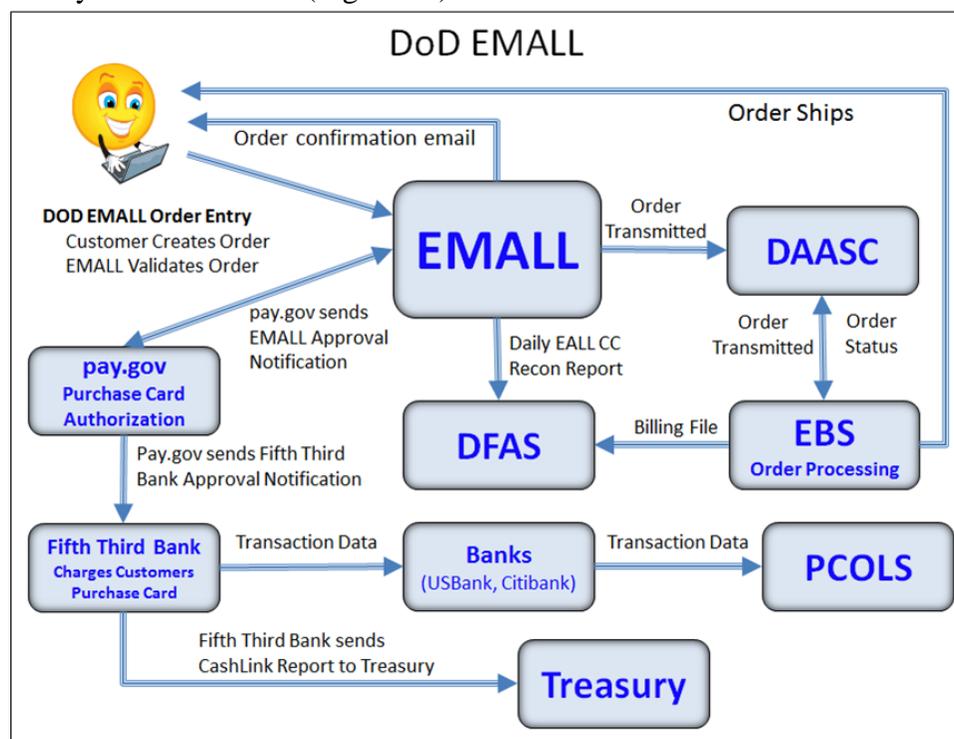


Figure 10: EMALL Process Flow

### 3.2 DoD 3-in-1 Tool

The DoD has numerous deployments to support various contingency and humanitarian requirements. Responding to these needs, DoD identified a requirement to improve the Micro-Purchase process when cash is used to pay for goods and services. There are three key processes for this type of cash purchase. These key processes are listed below:

1. Field Ordering,
2. Receiving, and
3. Payment.

To address these cash purchase needs, the department developed the 3-in-1 Tool. The 3-in-1 Tool automates the aforementioned three key processes into one solution. Formerly, these processes were accomplished with the Standard Form 44 (SF44) manual processes to purchase supplies and services used in contingency environments by a Field Ordering Officer (FOO) and Paying Agent (PA). The 3-in-1 Tool is used where GPC use is not feasible. The 3-in-1 Tool records cash and carry type purchases and payment data when conducting on-the-spot, over-the-counter, field cash purchases. This recorded purchase and payment data is then transmitted to the prime database for remote reconciliation and review. The 3-in-1 Tool is a joint procurement and financial management solution developed to reduce risk to the field team, improve procurement and cash management on the battlefield, and provide immediate visibility into purchases and payments.

The 3-in-1 Tool is comprised of three components, a ruggedized handheld device with portable printer, a workstation application, and a prime database/server. The handheld device is used in the field to input, temporarily store, and then transmit purchase and payment information. The small, ruggedized printer provides field print capability to document cash payments until data is uploaded. The workstation application is a hard client application that transmits data to the prime database/server (in a fully connected mode); stores a replica of the prime database for offline operations; and caches data from the device for later synchronization with the prime database/server. The prime database/server, a specialized module within the Joint Contingency Contracting System (JCCS), is an existing system used to manage and post contracts and track contractors housed at DISA (DECC). The 3-in-1 Tool prime database is used to manage devices and role-based system access; stores, reports, and analyzes purchase and payment data; and transmits payment information to other financial systems and order/voucher and receipt images for official document storage to Electronic Data Access (EDA).

Device, procurement, and financial management information is entered on the workstation by authorized personnel and then downloaded to the device to set it up for use by an assigned FOO and PA. FOO/PA is now able to process orders/payments on the device that can be immediately transmitted to the prime database/server for daily online review/clearance. Statuses of clearance and procurement/financial updates are transmitted back to the device as they are processed to update the device. Once orders have completed the review/clearance process, the Disbursing Agent can download and transmit payment information to the Deployable Disbursement System. Once the voucher number has been assigned, the prime database/server will transmit the SF44 and receipt image to EDA for official document storage.

Figure 11 provides the 3-in-1 Tool data flow.

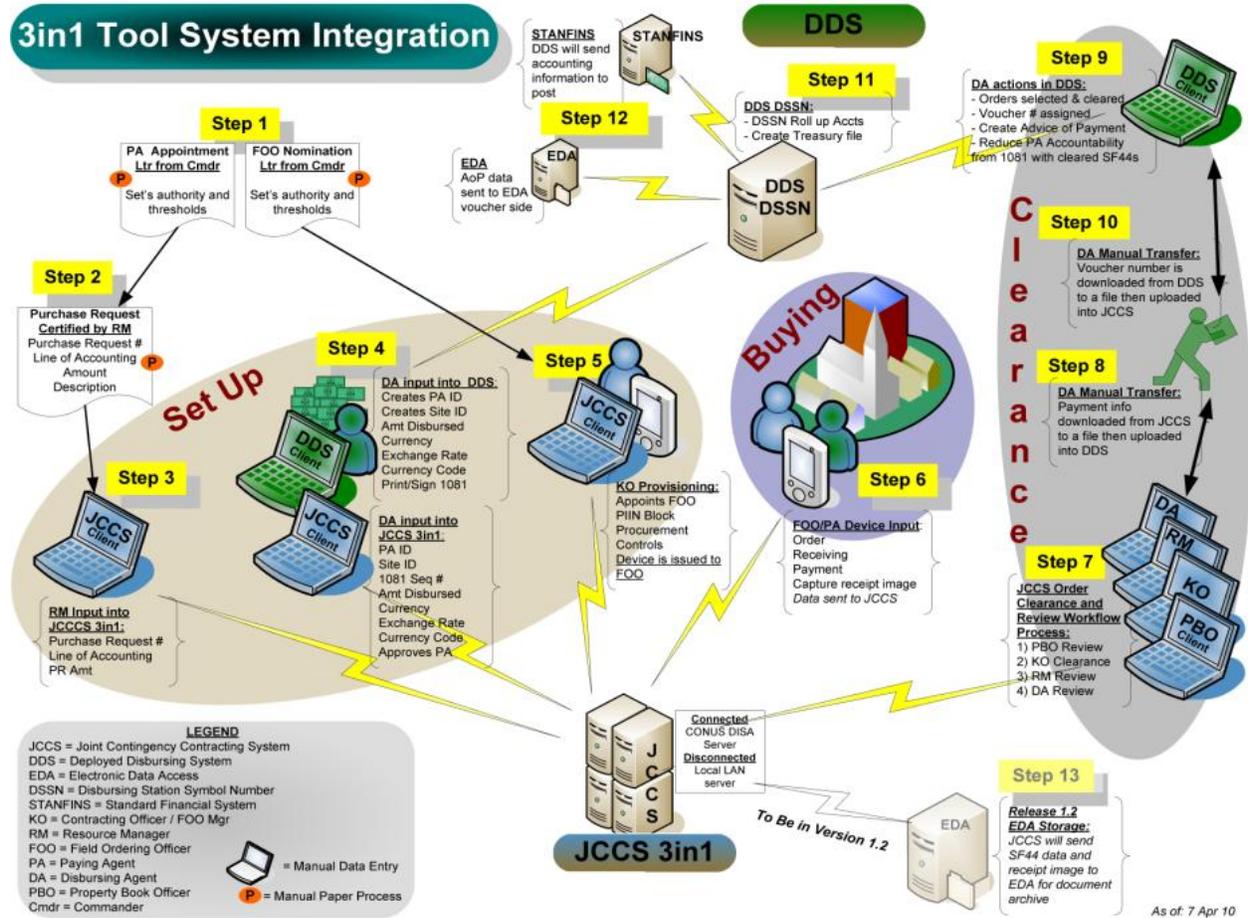


Figure 11: 3-in-1 Tool Data Flow

## 4.0 SUMMARY

This data management plan is a subset of an overarching Procurement Data Strategy under the governance of the Director of DPAP/PDI. The DoD GPC MP data is a complex and evolving ecosystem of people, the DoD, banks (to include the commercial card industry), GSA, and OMB-owned and controlled information systems. The GPC MP Program must be able to respond to data calls and queries from the DoD corporate level in a timely manner that provides sufficient transparency to acquisition metrics. The GPC MP Program must also implement and maintain internal controls and oversight of GPC Account usage. Increased data access and control will support investigation and audit support requests made by the Services.

Table 5. Streamlined Approach

Source	Content	Format	Final Recipient	Functional Use
U.S. Bank, Citibank, JPMorgan	Obligations/Invoices	ANSI X12	DFAS; Component Systems	Payment/Disbursement Rationale
U.S. Bank Citibank JPMorgan	Risk Predictive Model	Flat File; Custom	Data Mining/ Risk Analysis Vendor; TBD Analysis Org (DMDC)	Fraud detection; Enterprise Usage Metrics

By streamlining the data, DoD reduces the complexity and the storage/maintenance burden of retaining unused or little used data. The streamlined data is more readily exposed and aggregated with other procurement and acquisition data to provide coordinated, enterprise-level, business intelligence and acquisition dashboard information. Further, the RPM data includes the line-item detail (Level III) data when it is available.

### 4.1 Summary of Actions

[Table 6](#) provides a synopsis of the outstanding actions.

Table 6. Summary of Actions

#	Description	Completion Date	Section Number
2	To ensure PCOLS is used to manage card account issuance and maintenance, Risk Assessment needs to be enhanced to reflect appropriate risk when changes are made directly in the bank electronic automated system. This capability should follow behind line of accounting maintenance.	FY 2015	2.1.2
3	The DoD IG has recommended use of electronic retention of records. However, it has been requested that records retention be changed because of fraud and misuse in theater. Need resolution of this issue at Flag/SES level then publication of policy.	TBD	2.2.2
6	Begin requirements definition with Air Force NAF/JP Morgan Chase to establish feed for DM/RA	FY 2015	2.3.2

## APPENDIX A: OVERVIEW OF DEF/VCF FILE STRUCTURE

Appendix A - Synopsis of Daily transaction file contents			
DEF	Data Exchange File - Version 2008.1 dated 4/11/2008		
Transmitted by USBank and CitiBank			
	<b>Record</b>	<b>Contains</b>	<b>Purpose</b>
	0	00, 99	Header and Trailer
	1	31, 32, 03	Account Header, Extension
	2	30, 50, 7	Account transactions data - account summary, transactions. "Addendum" data - the industry-specific details and Level 3 data
	3	33	Account statement totals at monthly cycle
	4	19-22, 26	Hierarchy summaries - Company information = Approving/Billing Official
	5	37, 38,	Account information including authorization levels, MCC
	6	48, 49	authorization parameters, and address information
	7	null	Decline and Dispute transactions
	8	01, 05	Used to hold addendum data which is now carried at level 2
	9		Bank only - bank header and totals
			Reporting options
VCF	Visa Commercial Format 4.0 - Version 1.2 dated 3/6/2006		
Transmitted by USBank and JPMorganChase			
	<b>Record</b>		<b>Purpose</b>
		Header/Trailer	
	Type 1	Account Balance	Monthly at cycle; not on daily files
	Type 3	Card Account	Card Limits, status, balance due, past due,
	Type 4	Card Holder	Name, address, etc
	Type 5	Card Tx	Amount, MCC
	Type 6	Company info	Access Online Approving/Billing Officials hierarchy
	Type 7	Line Item Detail	Item Product Code, Commodity Code, Description, Qty, Unit cost
	Type 8	Line Item Summary	Discount, freight cost, source/destination
	Type 9	Lodging	Summary
	Type 10	Organization	Access Online ID and Node
	Type 11	Period	Billing period
	Type 14	Travel	Passenger Itinerary
	Type 15	Travel	Leg specific information
	Type 16	Supplier	DUNS, Location, TIN, SIC, Small Biz Class
	Type 26	Lodging	
	Type 28	Allocation	
	Type 29	Allocation Description	

## APPENDIX B: AF NAF RECONCILED DATA FORMAT

The data structure included in this Appendix is extracted from the Air Force Non-Appropriated Funds document that describes the requested interface for reconciled GPC data from JPMorgan Chase.

### Mapper Requirements

Table B-1. One Transaction Detail Record per Transaction

Field	Description	Start	Max Length	Format	Notes
A1	Record Type	1	1	VARCHAR	Constant "5"
A2	Account Number	2	16	VARCHAR	
A3	Post Date	18	10	VARCHAR	MMDDYYYY
A4	Transaction Date	28	10	VARCHAR	MMDDYYYY
A5	Merchant Name	38	25	VARCHAR	
A6	Source Currency	63	3	VARCHAR	Currency Code of Original Country - Example, USD or CAD
A7	Billing Currency	66	3	VARCHAR	Currency Code for Settlement Country - Example, USD
A8	Foreign Currency	69	15	VARCHAR	Original Currency Amount - no decimal, two places, right justified – zero fill, no sign indicator
A9	Foreign Currency Rate	84	5	VARCHAR	
A10	Reference Number	89	23	VARCHAR	
A11	MCC Code	112	4	VARCHAR	
A12	Transaction Amount	116	15	VARCHAR	Settlement Amount - no decimal, two places, right justified, zero filled, no sign indicator
A13	Transaction Code – DB/CR Indicator	131	2	VARCHAR	10 = Debit Amount 11 = Credit Amount
A14	Merchant City	133	26	VARCHAR	
A15	Merchant State	159	3	VARCHAR	
A16	Memo Flag	162	1	VARCHAR	The Memo Flag should indicate a Corporate or Individual Bill Account – If the transaction is a memo to the corporate bill statement then this is a C else I
A17	Merchant Country	163	3	VARCHAR	
A18	Merchant Zip	166	6	VARCHAR	
A19	Merchant Acquirer ID	172	8	VARCHAR	MMC_AcquiringMerchantID
A21	Processor Transaction Code	180	4	VARCHAR	TCO_Code
A25	Tax Included Code	184	1	VARCHAR	If the tax amount is not null, blank or zero then "Y" else "N"
A26	Tax Amount	185	11	VARCHAR	Tax Amount - no decimal, two places, right justified, zero filled, no sign indicator
A27	Transaction Authorization Number	196	6	VARCHAR	
Record Length:			202		

Table B-2. One Account Detail Record per Unique Account

<b>Field</b>	<b>Description</b>	<b>Start</b>	<b>Max Length</b>	<b>Format</b>	<b>Notes</b>
B1	Record Type	1	1	VARCHAR	Constant "2"
B2	Account Number	2	16	VARCHAR	
B3	Name	18	25	VARCHAR	Embossed Line1 on Card
B4	Address Line 1	43	36	VARCHAR	
B5	Address Line 2	79	36	VARCHAR	
B6	City	115	25	VARCHAR	
B7	State	140	2	VARCHAR	
B8	Zip	142	10	VARCHAR	
B9	Work Phone	152	10	VARCHAR	
B10	Company	162	5	VARCHAR	
B11	Level (TBR Hierarchy)	167	35	VARCHAR	
B12	Single Trans Limit	202	14	VARCHAR	
B13	Name Line 2	216	25	VARCHAR	
Record Length:			241		

Table B-3. One Merchant Record per Unique Merchant

<b>Field</b>	<b>Description</b>	<b>Start</b>	<b>Max Length</b>	<b>Format</b>	<b>Notes</b>
C1	Record Type	1	1	VARCHAR	Constant "7"
C2	Merchant Name	2	30	VARCHAR	
C3	Street	32	30	VARCHAR	
C4	City	62	20	VARCHAR	
C5	State	82	3	VARCHAR	
C6	Zip	85	9	VARCHAR	
C7	TIN	94	9	VARCHAR	Tax Payer Id Number
C8	Phone	103	15	VARCHAR	
C9	MasterCard 1099 Indicator	118	1	VARCHAR	
C10	MasterCard SBA Registered	119	1	VARCHAR	
C11	MasterCard SBA Disabled	120	1	VARCHAR	
C12	MasterCard Hub Zone	121	1	VARCHAR	
C13	MasterCard Veteran Indicator	122	1	VARCHAR	
C14	MasterCard Disabled Veteran Indicator	123	1	VARCHAR	
C15	MasterCard Vietnam Veteran Indicator	124	1	VARCHAR	
C16	MasterCard Information Refusal Indicator	125	1	VARCHAR	
C17	MasterCard Historically Black College Indicator	126	1	VARCHAR	
C18	MasterCard SBA Certified Business Indicator	127	1	VARCHAR	
C19	MasterCard Ethnicity of Business Owner	128	27	VARCHAR	
C20	MasterCard Gender Of Business Owner	155	1	VARCHAR	
C21	MasterCard Merchant Incorporation Status Code	156	16	VARCHAR	
C22	MasterCard EMR ID	172	50	VARCHAR	

## APPENDIX C: BANK EXTRACT FILE COMPARISON TO RPM

This Appendix documents the data elements captured from the Statement Billing File, or Reconciled Files, and populated into Oracle tables at DMDC. The Transaction and Account data provided GPC use information used by the DoD IG for investigation and audit. The Merchant data was the basis for DFAS to create IRS Forms 1099.

The data elements provided by each bank are listed and compared to each other. The Risk Predictive Model daily file is provided by banks in a common, single format. The data elements of the Risk Predictive Model that are equivalent to each Extract file data element are identified. Elements in a row are the same element provided by the source identified in the column heading. The number at the end of each message type (Transaction, Account, and Merchant) indicates the number of data elements provided by that source file. The number in the “%” column indicates the percentage of Reconciled File elements that are resident in the Risk Predictive Model file using the worst case (lowest percentage) bank source file.

Table C-1. Bank Extract File Comparison to RPM

	USBank Extract for DMDC	CitiBank Extract for DMDC	JP Morgan Chase Extract for DMDC	Risk Predictive Model	%
<b>TRANSACTIONS:</b>				In "Transaction" Section unless notes in paren	
	TYPE_CD position(1-1),	TYPE_CD position(1-1),	Record Type (5=transaction)		
	ACCT position(2-17),	ACCT position(2-17),	Account Number	CA_ACCT_NUM (Main)	
	PDATE position(18-25),	PDATE position(18-25),	Post Date	TX_POST_DATE	
	TDATE position(26-33),	TDATE position(26-33),	Transaction Date	TX_AUTH_DATE	
	MERDS position(34-58),	MERDS position(34-58),	Merchant Name	TX_MRCH_NAME	
	SCURC position(59-61),	SCURC position(59-61),	Source Currency	TX_SRC_CURR_CD	
	BCURC position(62-64),	BCURC position(62-64),	Billing Currency	TX_BILL_CURR_CD	
	FCURA position(65-77),	FCURA position(66-79),	Foreign Currency	TX_SRC_AMT	
	REFN position(78-100),	REFN position(80-102),	Reference Number	TX_REFERENCE_NBR	
	SIC position(101-104),	SIC position(103-106),	MCC Code	TX_MCC	
	TAMT position(105-117),	TAMT position(108-121),	Transaction Amount	TX_BILL_AMT	
	VTCOD position(118-119),	VTCOD position(122-123),	DR/CR indicator	TX_DB_CR_IND	
	MCITY position(120-145),	MCITY position(124-149),	Merchant City	TX_MRCH_CITY	
	MSTAT position(146-148),	MSTAT position(150-152),	Merchant State	TX_MRCH_STATE	
	TMEMO position(149-149),	TMEMO position(240-240),	Corp or Individual Account	CA_ISSUE_TYPE (Card-Set up)	
	MCTRY position(153-155),	MCTRY position(157-159),	Merchant Country	TX_MRCH_CNTRY	
		TICK position(178-190),			
	MZIP position(156-161),	MZIP position(191-195),	Merchant Zip	TX_MRCH_POSTAL_CD	
	MACQN position(162-169),	MACQN position(160-165),	Merchant Acquirer ID	TX_ACQ_ID	
		MACCT position(241-255),			
	MSP_ID position(170-185),	MSP_ID position(241-255),		TX_MRCH_ID	
	MIDF position(186-210),	MIDF position(215-239),			
	TRCOD position(211-214),		Processor Transaction Code	TX_TRAN_CD	
	PCOD position(215-215),				
	PID position(216-240),	PID position(215-239),		TX_PURCHASE_ID	
	TXCOD position(241-241),		Tax Included Code	TX_US_TAX_FLAG	
	TAX position(242-250),	TAX position(204-214),	Tax Amount	TX_US_TAX_AMT	
	AUTH position(251-256)	AUTH position(261-266)	Transaction Authorization Number	TX_AUTH_CODE	
			Foreign Currency Rate		
	25	24	22	23	92%

	USBank Extract for DMDC	CitiBank Extract for DMDC	JP Morgan Chase Extract for DMDC	Risk Predictive Model	%
<b>ACCOUNTS:</b>			Record Type (Account = 2)		
	ACCT position(2-17),	ACCT position(40-55),	Account Number	CA_ACCT_NUM (Main)	
	NAME position(18-42),	NAME position(82-106),	Name	Not transmitted from bank with RPM data	
	ALIN2 position(67-101),	ALIN2 position(158-193),	Address Line 2	CA_ADDR_LNE2	
	UACCT3 position(145-158),				
	COMPANY position(145-149),	COMPANY position(354-358),	Company	HL_PROC_COMPANY (Processing Hier)	
	CRATE position(173-174),			CA_CR_RATING_CD	
	ALIN1 position(175-210),	ALIN1 position(122-157),	Address Line 1	CA_ADDR_LINE1	
	CITY position(211-235),	CITY position(194-218),	City	CA_CITY	
	STATE position(236-237),	STATE position(219-220),	State	CA_STATE	
	ZIP position(238-246),	ZIP position(221-229),	Zip	CA_POSTAL_CD	
	WPHONE position(247-256),	WPHONE position(344-353)	Work Phone	Not transmitted from bank with RPM data	
	LEVL position(258-292),	LEVL position(5-39),	Level (TBR Hierarchy)	HL_TBR_ORG, SERVICE, MCOM, REGION, INSTALL, MA, CH (main)	
	SVC position(266-267),			SERVICE	
	CARD_TYPE position(317-317),	CARD_TYPE position(56-56),		CA_ISSUE_TYPE (?)	
	NAME2 position(397-421),	NAME2 position(107-121),	Name Line 2	Not transmitted from bank with RPM data	
	STRANS_LMT position(422-436),	STRANS_LMT position(380-394),	Single Trans Limit	CA_TRAN_LIM and AIM_CA_TRAN_LIM (from AIM)	
	MTRANS_LMT position(437-451)	MTRANS_LMT position(231-239),		CA_CYCLE_LIM	
		ID_VER position(315-316),			
	17	15	12	13	76%

	USBank Extract for DMDC	CitiBank Extract for DMDC	JP Morgan Chase Extract for DMDC	Risk Predictive Model	%
<b>MERCHANTS:</b>				In Transaction section	
			Record Type (7=Merchant)		
	M_LEGAL_NAME position(1-30),	M_LEGAL_NAME position(69-138)	Merchant Name	TX_MRCH_NAME	
	M_LOC_NAME position(31-60),			TX_MRCH_ID	
	M_ALT_NAME position(61-90),	M_DBA_NAME position(140-161),			
	M_STREET position(91-120),	STREET position(163-222),	Street		
	M_CITY position(121-140),	CITY position(224-253),	City	TX_MRCH_CITY	
	M_STATE position(141-143),	STATE position(255-256),	State	TX_MRCH_STATE	
	M_ZIP position(144-152),	ZIP position(262-271),	Zip	TX_MRCH_POSTAL_CODE	
	DUNS position(153-161),				
	M_INC position(162-163),	INC position(290-339),	Mastercard Merchant Incorporation Status		
	M_MINORITY_CD position(164-166),	MINORITY position(341-341),	Mastercard Ethnicity of Business Owner		
	TIN position(166-174),	TIN position(345-359),	TIN		
	M_PHON position(175-189),	PHONE position(273-288),	Phone		
	PROP_FIRST_NAME position(190-215),	PROP_FIRST_NAME position(485-495),			
	PROP_M_INITIAL position(215-215),				
	PROP_LAST_NAME position(216-216),	PROP_LAST_NAME position(497-510),			
	M_WOMAN_OWNED position(243-243),	WOMAN_OWNED position(343-343),	Mastercard Gender of Business Owner		
	MCC position(243-246),	MCC position(13-16),		TX_MCC	
	MSP_ID position(247-261),	MERCH_ID position(1-11),			
	ALT_CITY position(273-292),				
	ALT_STATE position(293-295),				
	ALT_ZIP position(296-304),				
	TIN_TYPE position(320-320),				
	M_SALES position(321-330),	SALES position(463-471),			
	M_NBR_EMPL position(331-336),	NBR_EMPL position(474-482),			
	M8A_CLASS position(337-337),	M8A_CLASS position(512-512),			
	M8A_EXP position(338-347),				
	SBA_PART position(348-348),	SBA_PART position(514-514),	Mastercard SBA Registered		
	DIS_VET position(349-349),	DIS_VET position(516-516),	Mastercard Disabled Veteran Indicator		
	VET position(350-350),	VET position(518-518)	Mastercard Veteran Indicator		
	VIET_VET position(351-351),		Mastercard Vietnam Veteran Indicator		
	REFUSAL position(352-352)		Mastercard Information Refusal Indicator		
		M_COUNTRY position(258-260),		MRCH_CNTRY	
		MCC_DESCR position(18-67),			
			Mastercard 1099 Indicator		
			Mastercard SBA Disabled		
			Mastercard HUB Zone		
			Mastercard Historically Black College Ind		
			Mastercard SBA Certified Business Ind		
			Mastercard EMR ID		
	31	23	21	7	22%

## APPENDIX D: RISK PREDICTIVE MODEL DAILY FILE

This Appendix is the specification of the daily data feed expected by Data Mining from the banks aggregated with the data from PCOLS. Cells highlighted in red reflect elements that are anticipated by Data Mining, but are not transmitted (and have no placeholder in current file structure) from PCOLS.

*This Appendix has been redacted, and is considered sensitive.*

## APPENDIX E: RISK PREDICTIVE MODEL MONTHLY FILE

This Appendix is the specification of the monthly data used by the DM/RA contractor. These files are provided by the Banks.

*This Appendix has been redacted.*

## APPENDIX F: ACRONYMS AND ABBREVIATIONS

Table F-1. Acronyms and Abbreviations

<b>Acronym/ Abbreviation</b>	<b>Definition</b>
A/OPC	Agency/Organization Program Coordinator
A/BO	Approving/Billing Official
AF	Air Force
AIM	Authorization Issuance and Maintenance
ANSI	American National Standards Institute
ABO	Approving/Billing Official
BI	Business Intelligence
CAC	Common Access Card
CCF	Citibank Commercial File
CERS	Citibank Electronic Reporting System
COOP	Continuity of Operations
CRCARD	Pseudo Pay DODAAC for routing purchase acceptance transactions
DAASC	Defense Automated Addressing System Center
DAU	Defense Acquisition University
DEERS	Defense Enrollment and Eligibility System
DEF	Data Exchange File
DFAS	Defense Finance and Accounting Service
DISA	Defense Information Systems Agency
DM/RA	Data Mining/Risk Assessment
DMDC	Defense Manpower Data Center
DOD	Department of Defense
DODAAC	Department of Defense Activity Address Code
DPAP	Defense Procurement and Acquisition Policy
EMMA	Enterprise Monitoring and Management of Accounts
FAR	Federal Acquisition Regulation
FICO	Fair Isaac Corporation
FMR	Financial Management Regulation
GAO	Government Accountability Office
GEX	Global Exchange
GPC	Government Purchase Card
GSA	General Services Administration
HNC	HNC Software Inc., HNC merged with FICO in 2002
IG	Inspector General
JOQ	Joint Organizational Query
NAF	Non-Appropriated Funds
NITC	NAVFAC Information Technology Center
OMB	Office of Management and Budget
OPTI	Obligation Processing Type Indicator
PAT	Program Audit Tool
PCOLS	Purchase Card Online System

<b><i>Acronym/ Abbreviation</i></b>	<b><i>Definition</i></b>
PCPO	Purchase Card Policy Office
PDI	Program Development and Implementation
PDF	Portable Document Format
RPM	Risk Predictive Model
SALTS	Standard Automated Logistics Tool Set
SBF	Statement Billing File
SIC	Standard Industrial Classification
SRS	Sign-on and Referral System
TBD	To Be Determined
TBR	Total Business Reporting
TIN	Taxpayer's Identification Number
TRP	Tax Reporting Program
TSYS	Total System Services, Inc.
UDF	User Defined File
USD	United States Dollar
VCF	VISA Commercial File
WAWF	Wide Area Workflow
XML	Extensible Markup Language