Report No. DODIG-2012-087 May 29, 2012

Inspector General
United States Department of Defense

Logistics Modernization Program System Procure-to-Pay Process Did Not Correct Material Weaknesses

Additional Copies

To obtain additional copies of this report, visit the Web site of the Department of Defense Inspector General at http://www.dodig.mil/audit/reports or contact the Secondary Reports Distribution Unit at (703) 604-8937 (DSN 664-8937) or fax (571) 372-7469.

Suggestions for Audits

To suggest or request audits, contact the Office of the Deputy Inspector General for Auditing by phone (703) 604-9142 (DSN 664-9142), by fax (571) 372-7469, or by mail:

Department of Defense Office of Inspector General
Office of the Deputy Inspector General for Auditing
ATTN: Audit Suggestions/13F25-04
4800 Mark Center Drive
Alexandria, VA 22350-1500

DEPARTMENT OF DEFENSE
hotline

To report fraud, waste, mismanagement, and abuse of authority.

Send written complaints to: Defense Hotline, The Pentagon, Washington, DC 20301-1900
Phone: 800.424.9098 e-mail: hotline@dodig.mil www.dodig.mil/hotline

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

May 29, 2012

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE (COMPTROLLER)/
CHIEF FINANCIAL OFFICER, DOD
DEPUTY CHIEF MANAGEMENT OFFICER
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: Logistics Modernization Program System Procure-to-Pay Process Did Not Correct Material Weaknesses (Report No. DODIG-2012-087)

We are providing this final report for your review and comment. This report addresses the Army's implementation of one of the DoD Business Enterprise Architecture end-to-end business processes within the Logistics Modernization Program system. Despite spending about $1.8 billion, Army managers did not accomplish the reengineering needed to integrate the Procure-to-Pay functions to comply with DoD Business Enterprise Architecture requirements and correct material weaknesses. We considered management comments on a draft of this report when preparing the final report.

DoD Directive 7650.3 requires that recommendations be resolved promptly. We received comments from the Deputy Chief Management Officer and the Assistant Secretary of the Army (Financial Management and Comptroller). The Deputy Chief of Management Officer comments were responsive, and no further comments are needed. The Assistant Secretary of the Army (Financial Management and Comptroller) comments, sent on behalf of the Department of the Army, were generally responsive. However, comments to Recommendations C.2.b and C.2.c were nonresponsive and comments on Recommendations A.1.a, A.1.e, A.1.f, A.1.g, A.1.h, A.1.i, B.1.a, and C.2.a were partially responsive. We request additional comments from the Assistant Secretary of the Army (Financial Management and Comptroller) and Army Office of Business Transformation on the recommendations by June 28, 2012.

If possible, send a portable document format (.pdf) file containing your comments to audfmr@dodig.mil. Copies of your comments must have the actual signature of the authorizing official for your organization. We are unable to accept the /Signed/ symbol in place of the actual signature. If you arrange to send classified comments electronically, you must send them over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Please direct questions to me at (703) 604-8938 (DSN 664-8938).

Richard B. Vasquez

Richard B. Vasquez, CPA
Acting Assistant Inspector General
Financial Management and Reporting

Report No. DODIG-2012-087 (Project No. D2010-D000FI-0234.000) May 29, 2012

Results in Brief: Logistics Modernization Program System Procure-to-Pay Process Did Not Correct Material Weaknesses

What We Did

Our objective was to determine whether appropriate internal controls were in place within the Logistics Modernization Program system (LMP) to ensure proper recording of accounting transactions related to the purchase of goods and services.

What We Found

Army financial and system managers did not reengineer LMP to perform Procure-to-Pay functions correctly or correct known material weaknesses. The LMP developers did not identify the system requirements needed to correct the root causes of material weaknesses, and Army managers did not review control activities to assess internal control effectiveness. As a result, Army managers continued the use of costly business processes and LMP failed to provide reliable financial data. As of August 31, 2011, LMP activities reported more than $10.6 billion in abnormal balances within the Procure-to-Pay general ledger accounts.

LMP system access controls did not establish data integrity for the Procure-to-Pay process because Army managers did not provide effective oversight over the development and implementation of system access templates. As a result, LMP data were at risk of unauthorized and fraudulent use. In addition, the Army Enterprise Systems Integration Program Management Office did not determine the Standard Financial Information Structure data attributes needed to establish the vendor master database and populate the correct domain values for Army systems to process Procure-to-Pay transactions correctly. This occurred because Army managers did not create the single source of vendor master data needed to develop, manage, and maintain trading partner information. As a result, the Army allotted about $1.3 million to develop vendor information for two systems but did not resolve material weaknesses related to accounts payable and intragovernmental eliminations.

What We Recommend

The Deputy Chief Management Officer should review legacy registration processes to determine whether DoD can incorporate registry databases into the System for Award Management. Other recommendations are:

- develop a plan of action and milestones to bring the LMP into compliance with the DoD requirements,
- modify LMP to cease the automatic obligation of unmatched disbursements,
- review unobligated balances, and
- develop a system edit check to identify activity exceeding allotted amounts.

The Army should also create and manage vendor master data based on the System for Award Management and establish a vendor master data manager. Further, the Army should improve LMP system access controls and assess the LMP Procure-to-Pay business process.

Management Comments and Our Response

The Deputy Chief Management Officer and Department of the Army agreed with our recommendations. However, some of the Army comments were not responsive or did not fully address what actions it would take to correct the reported deficiencies. Therefore, we request that the Army provide additional comments as specified in the recommendations table on the back of this page.

Recommendations Table

Management	Recommendations Requiring Comment	No Additional Comments Required
Deputy Chief Management Officer		C.1
Assistant Secretary of the Army (Financial Management and Comptroller)	A.1.a, A.1.e, A.1.f, A.1.g, A.1.h, A.1.i, B.1.a, C.2.a, C.2.b, C.2.c	A.1.b, A.1.c, A.1.d, A.2.a, A.2.b, A.2.c, A.3, B.1.b, B.1.c, B.1.d, B.1.e, B.1.f, B.2.a, B.2.b, B.2.c, C.4
Director, Army Office of Business Transformation	A.1.a, A.1.e, A.1.f, A.1.g, A.1.h, A.1.i, C.2.a, C.2.b, C.2.c	A.1.b, A.1.c, A.1.d
Program Manager, Army Enterprise Systems Integration Program		C.3.a, C.3.b, C.3.c, C.3.d

Please provide comments by June 28, 2012.

Table of Contents

Introduction 1

Objective 1
Material Weaknesses Related to Business Processes and Systems 1
DoD Procure-to-Pay Process 1
Review of Internal Controls Over the Business Process 3

Finding A. Logistics Modernization Program Procure-to-Pay Reengineering Did Not Correct Known Weaknesses 4
Army Procure-to-Pay Responsibilities 4
Army Managers Did Not Implement the Business Enterprise Architecture Business Process 5
Developing an Effective Control Environment 6
Implementing Control Activities to Accomplish Procure-to-Pay Business Process 8
Ineffective Monitoring of the Army Procure-to-Pay Business Process 18
Conclusion 19
Recommendations, Management Comments, and Our Response 19

Finding B. Logistics Modernization Program System Access Controls Were Ineffective 26
System Compliance with Federal Information Security Management Act 26
Segregation of Duties and Least Privilege Controls 27
Developing Consistent Account Management Policy and Procedures 31
Army Materiel Command Taking Actions to Update Account Management 35
Conclusion 36
Recommendations, Management Comments, and Our Response 37

Finding C. Vendor Master Data Did Not Support the Procure-to-Pay Process 41
Vendor Master Information Requirements 41
Developing a Single Army Vendor Master 43
Army Expended Funds to Develop Multiple Vendor Tables 47
Developing a Way Forward 48
Conclusion 48
Recommendations, Management Comments, and Our Response 49

Appendices
A. Scope and Methodology 54
B. Prior Coverage 56
C. Description of Technical Requirements and Standards 57
D. Acronyms and Abbreviations 60
E. Business Transformation Agency Procure-to-Pay Illustration 61
F. Segregation of Duties 63
G. Statistical Sampling Methodology 66

Table of Contents (cont'd)

Appendices (cont'd)

H. Developing the Vendor Master Using Standard Financial Information Structure Attributes 69

Glossary 71

Management Comments

Deputy Chief Management Officer 72

Department of the Army 74

Introduction

Objective

Our overall objective was to determine whether the appropriate internal controls were in place within the Logistics Modernization Program system (LMP) to ensure the proper recording of accounting transactions related to the purchase of goods and services. Specifically, we determined the reasons for abnormal account balances[1] and transaction relationships and determined whether LMP properly supported the accounting transactions within the general ledger accounts with verifiable audit trails. This report assesses the Army's implementation of the DoD Business Enterprise Architecture (BEA) end-to-end business process for Procure-to-Pay (P2P) in LMP. See Appendix A for a discussion of our scope and methodology and Appendix B for prior audit coverage. See Appendix C for the description of technical requirements and standards and Appendix D for acronyms and abbreviations. See the Glossary for definitions of technical terms used in this report.

Material Weaknesses Related to Business Processes and Systems

The Army has long-standing material weaknesses in the financial reporting of its Army Working Capital Fund (AWCF) business operations. The Army did not design its legacy accounting systems to collect and record financial information using accrual accounting or to maintain auditable data at the transaction level to support the amounts reported on the AWCF financial statements. In its FY 2010 Statement of Assurance, the Army reported 10 material weaknesses related to its AWCF business processes and systems. The material weaknesses involving accounts payable, abnormal balances (both discussed in Finding A), and intergovernmental eliminations (discussed in Finding C) related directly to the P2P business process. These three material weaknesses existed because of the inability of Army legacy systems to integrate the P2P business process correctly and identify the proper trading partner information for Federal and non-Federal transactions. Appendix C contains the definition of a material weakness and a detailed description of the three material weaknesses. In the Army's FY 2011 Statement of Assurance, the Assistant Secretary of the Army (Financial Management and Comptroller) (ASA[FM&C]) identified LMP deployment as the major corrective action for resolving these three material weaknesses.

DoD Procure-to-Pay Process

The Deputy Chief Management Officer (DCMO) had overall responsibility for developing and ensuring the implementation of the DoD BEA requirements. The Under Secretary of Defense (Comptroller)/Chief Financial Officer is responsible for ensuring that the Army complies with financial reporting requirements.

---

[1] An abnormal balance occurs when the balance reported in a general ledger account is different from the expected normal balance for that account as defined in the chart of accounts. For example, the normal balance for accounts payable (GLAC 2110) is a credit balance. When the trial balance reports the value as a debit balance, the balance is considered abnormal.

DoD developed the BEA to assist its components in developing the common end-to-end business processes needed to report the financial and other data managers need for decision-making. The BEA supports the move from a function-centered approach to one that looks at DoD business functions across the enterprise from an end-to-end process perspective. BEA version 7.0, released on March 12, 2010, introduced the end-to-end business flows to serve as the foundation for a shared understanding of the target architecture. The BEA provided the business rules and transactional information flows needed to develop Enterprise Resource Planning (ERP) system solutions. The P2P business process was one of 15 BEA end-to-end business processes. Additional details about the BEA P2P business process are in Appendix E.

DoD Responsibilities

The DCMO issued guidance on October 13, 2009, restating the Defense Business Systems Management Committee's commitment to explore the execution of the P2P end-to-end business process entirely within the ERP systems to the maximum extent possible, using pilots programs. The FY 2010 National Defense Authorization Act (the Act), Section 1072, introduced new requirements into the Department's investment review process. The Act stipulated that DoD could not certify Defense business system modernization funds in excess of $1 million for obligation without making a determination on whether or not DoD had conducted appropriate business process reengineering of the system processes. To justify additional LMP funding, the Act required the DCMO and the Army's Chief Management Officer to make the reengineering determinations.

The DCMO issued a memorandum dated February 12, 2010, implementing Section 1072 of the Act. The memorandum required the completion of an interim Business Process Reengineering Assessment Form by the Chief Management Officer of ERP systems coming to the DoD Investment Review Board (the Board). In September 2010, the Board granted a third LMP deployment decision, which included more than $37 million for the Army to continue deployment and related support activities. The Board issued an Acquisition Decision Memorandum dated November 18, 2010, acknowledging that the Army knew risks existed in the system before deployment that must be mitigated in future software releases of LMP. The Acquisition Decision Memorandum provided seven specific tasks that needed to occur, including the requirement for Army managers to ensure that they executed all future capability upgrades in accordance with an approved strategy for the emerging Army ERP systems.

Logistics Modernization Program System

In December 1999, the Program Director, U.S. Army Wholesale LMP, Army Materiel Command (AMC), awarded a service contract to develop and deploy LMP to process logistical and financial data in support of AWCF business operations and to maintain legacy systems until full LMP deployment. The contractor used a commercial off-the-shelf software package to develop the LMP financial management and logistics functionality. In July 2003, the LMP Project Office initially deployed LMP to the CECOM Life Cycle Management Command (LCMC), New Jersey; Tobyhanna Army Depot, Pennsylvania; Defense Finance and Accounting Service (DFAS) locations in Indianapolis, Indiana, and Columbus, Ohio; and several other AMC activities supporting the AWCF Supply Management business area. In May 2009, the LMP Project Office completed its second deployment to an additional seven AMC locations, including the Aviation and Missile Command LCMC, Alabama (the LCMC) and Letterkenny Army Depot

Pennsylvania (the Depot) that we visited. The LMP Project Office completed deployment to the remaining AWCF activities on October 21, 2010. During FY 2011, 28 AWCF activities used LMP to report trial balance data. DoD Inspector General (DoD IG) Report No. D-2011-015, "Insufficient Governance Over Logistics Modernization Program System Development," November 2, 2010, reported that LMP had not resolved any previously reported material weaknesses, despite the Army spending more than $1.1 billion to develop and deploy the system. As of July 2011, the Army spent about $1.8 billion on LMP. In December 2011, the Army issued a contract modification for almost $1 billion to extend the existing contract until December 2015.

Standards for Internal Control

Office of Management and Budget Circular No. A-123, "Management's Responsibility for Internal Control," December 21, 2004, and Government Accountability Office (GAO) "Standards for Internal Control in the Federal Government," November 1999, identify the standards and policies for achieving proper internal control. The circular provides Federal managers with guidance to ensure that they establish effective internal control standards. Management must also comply with the circular's Appendix A, "Internal Control Over Financial Reporting," when assessing internal control effectiveness over financial reporting. Effective internal controls provide management with reasonable assurance of effective and efficient operations, reliable financial reporting, and compliance with laws and regulations. The five standards of internal control are defined in Appendix C.

Review of Internal Controls Over the Business Process

DoD Instruction 5010.40, "Managers' Internal Control Program (MICP) Procedures," July 29, 2010, requires DoD organizations to implement a comprehensive system of internal controls that provides reasonable assurance that programs are operating as intended and to evaluate the effectiveness of the controls. We identified internal control weaknesses in the management and implementation of the LMP P2P business process. Specifically, Army financial managers did not properly reengineer AWCF business processes and implement internal control procedures for conducting the LMP P2P business process, correctly administer LMP system access, or properly develop the vendor master data needed to associate financial data to the correct trading partners. We will provide a copy of the report to the senior officials responsible for internal controls in the Department of Army.

Finding A. Logistics Modernization Program Procure-to-Pay Reengineering Did Not Correct Known Weaknesses

ASA(FM&C) and AMC managers developed LMP business processes to perform LMP P2P functions that did not implement the DoD BEA requirements and correct known material weaknesses. Specifically, the LMP processes developed did not properly approve, verify, or reconcile P2P transactions or record and document business events accurately. This occurred because the managers did not:

- develop an effective control environment to identify the root causes of the material weaknesses related to the P2P business process, develop appropriate corrective actions, and reengineer the Army business processes and LMP system functionality to resolve the weaknesses;
- establish the LMP control activities needed to accomplish the P2P business process requirements; and
- monitor operations within the LMP P2P business process.

As a result, Army managers continued the use of costly legacy business processes and LMP failed to provide reliable data to financial managers, which may impede an AWCF audit opinion by FY 2017. As of August 31, 2011, LMP activities reported more than $10.6 billion in abnormal balances within the accounts payable and budgetary general ledger accounts supporting the P2P business process. LMP also continued to create and automatically obligate unmatched disbursements, [2] requiring the Army and DFAS to expend additional funds and resources to accomplish the manual reconciliation processes needed to post disbursements correctly.

Army Procure-to-Pay Responsibilities

The Deputy Assistant Secretary of the Army (Financial Operations) reports to the ASA(FM&C) and has responsibility for policies, procedures, programs, and systems pertaining to finance and accounting activities and operations. The Deputy Assistant Secretary of the Army (Financial Operations) also has responsibility for implementing Army financial management systems, data integration, and the Army internal control program. ASA(FM&C) had responsibilities for ensuring that LMP, as the AWCF's ERP system, correctly implemented these business flows before allowing the LMP Project Manager to fully deploy the system. As reported in DoD IG Report No. D-2011-015, the ASA(FM&C) was not sufficiently involved in LMP development and did not identify LMP financial management problems that required immediate corrective actions before LMP full deployment. Specifically, AMC personnel developed a majority of the requirements for the LMP P2P business process.

[2] An unmatched disbursement is a disbursement transaction that has been received and accepted by an accounting office, but has not been matched to the correct detail obligation. This includes transactions that have been rejected and returned back to the paying office or central disbursement clearing organization by an accounting office.

On February 5, 2010, the Secretary of the Army signed General Order 2010-01, establishing the Army Office of Business Transformation (OBT). The order stated that the Army had originally established the Army OBT by memorandum on April 9, 2009. The Army OBT acts under the authority, direction, and control of the Secretary of the Army; reports directly to the Army Chief Management Officer; and is the lead for business transformation efforts Army-wide. Both the OBT and ASA(FM&C) now share the responsibility for ensuring that LMP activities implement the appropriate internal control over the financial business processes.

Army Managers Did Not Implement the Business Enterprise Architecture Business Process

The Army Director, OBT; ASA(FM&C); and AMC financial and system managers (hereafter referred to collectively as Army managers) did not develop an LMP P2P business process that complied with DoD BEA requirements. The BEA required that an ERP system demonstrate its adherence to the 15 BEA business processes and related business rules as well as DoD Financial Management Improvement Guidance, Federal accounting standards, and applicable public laws such as the Federal Financial Manager's Integrity Act of 1996, regulations, and policies governing the business process. Specifically, systems must comply with the Federal Financial Management System Requirements as required by Office of Management and Budget Circular No. A-127, "Financial Management Systems," January 9, 2009, and the Financial System Integration Office's Core Financial System Requirements.

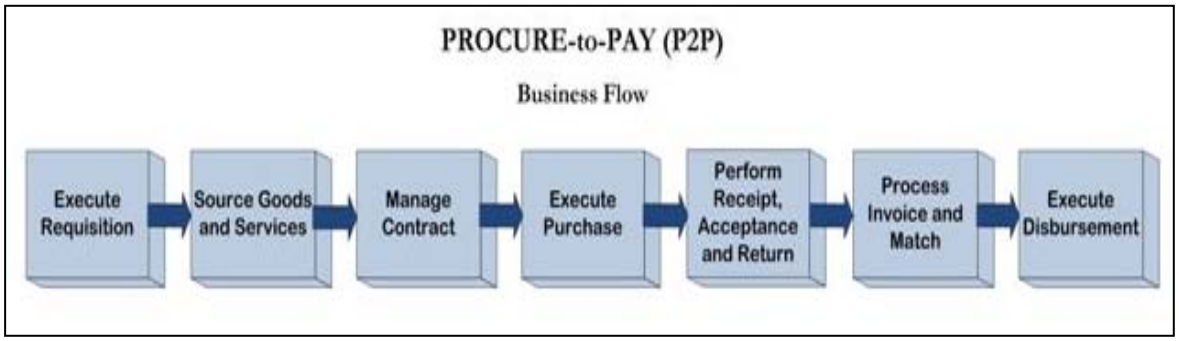
When the Army initially deployed LMP in July 2003, the 15 BEA business processes had not been identified. In FY 2005, the Business Transformation Agency (BTA) began developing the BEA P2P business process. ASA(FM&C) and AMC managers developing LMP had not assessed what impact emerging BEA requirements had on further LMP deployment. They also did not determine whether they needed to delay deployment and ensure that they conducted the appropriate business process reengineering needed to integrate the LMP P2P business process at full deployment. As a result, they did not provide the LMP Project Office with the correct requirements needed to develop the LMP functionality needed to meet the requirements of the BEA P2P business process. Instead, Army managers made the decision to delay business process reengineering until after LMP had deployed and sought the Board's approval to continue deployment in September 2010. The Board decided to allow the Army to fully deploy LMP without first ensuring that the Army managers had reengineered LMP P2P business process to resolve the material weaknesses that had existed in the legacy environment.

ASA(FM&C) and AMC managers developing LMP had not assessed what impact emerging BEA requirements had on further LMP deployment.

Army OBT and ASA(FM&C) managers did not take advantage of the Defense Business Systems Management Committee's commitment to explore the execution of the P2P business process within LMP. They did not direct the LMP Project Office to reengineer the legacy environment to the extent necessary to develop a LMP P2P business process that would ensure the appropriate AWCF personnel approved, verified, or reconciled P2P transactions and recorded and documented the financial transactions and business events accurately. The legacy environment that these Army managers largely perpetuated within LMP consisted of multiple nonintegrated systems performing specific functions within the P2P business process. Appendix E compares

the BEA requirements for the P2P business process to the "as is" environment for obtaining goods and services. Figure 1 shows the P2P business flow related to the six phases of the BEA P2P business process: Requisitioning and Commitments (Execute Requisition), Contracting and Obligations (Source Goods and Services, Manage Contract, and Execute Purchase), Goods Receipt (Perform Receipt, Acceptance and Return), Invoicing (Process Invoice and Match), Entitlement (Process Invoice and Match), and Disbursing (Execute Disbursement).

Figure 1. Business Enterprise Architecture, Version 7.0, P2P Business Flow



Source: DoD BEA, Version 7.0

Developing an Effective Control Environment

Army managers did not develop an effective control environment to identify the root causes of the material weaknesses related to the P2P business process, develop appropriate corrective actions, and reengineer the Army business processes. This prevented the LMP Project Office from designing the final LMP business process correctly by taking advantage of the inherent capabilities contained in the commercial software for accomplishing the P2P business process. Army managers also did not analyze the root causes for known material weaknesses within the current P2P business process to design and implement the corrective actions needed to resolve the weaknesses. Consequently, they instructed the LMP Project Office to configure LMP to perpetuate AMC legacy business processes. This configuration resulted in a non-integrated P2P business process that could not resolve the material weaknesses related to accounts payable, abnormal account balances, and intragovernmental eliminations.

Control Environment Resulted in Additional Costs to Maintain Legacy Systems and Processes

ASA(FM&C) did not ensure that AMC personnel designed LMP requirements that would implement the commercial software's full P2P capabilities. Therefore, AMC personnel did not reengineer LMP to provide the integration required to perform all phases of the P2P business process. Soon after the July 2003 LMP deployment, Army managers should have assessed its business operations, identified all existing P2P business processes and systems used in the legacy environment and the commercial software capabilities to accomplish these business processes, and developed a reengineering plan to integrate these processes within LMP. If ASA(FM&C)

had instructed the LMP program managers to reengineer the LMP P2P business process, then DFAS and LMP activities could have discontinued the use of costly legacy business processes and systems to accomplish the P2P business process. For example:

- At the Depot, personnel continued to use the Aquiline system to create purchase requests to solicit and award service contracts. Aquiline is a commercial Purchase Request software tool used by AMC contracting activities. Resource managers entered a purchase request in Aquiline before the requisition information was manually entered into LMP because LMP lacked the internal controls and functionality needed for online approval and funds certification. The Army did not integrate the Aquiline system into LMP or any other financial management system. The Army planned to retire the Aquiline system after the Army deployed both LMP and the Army General Fund Enterprise Business System (GFEBS). In July 2011, the Army extended the use of Aquiline with the potential additional cost of $1.1 million for its use during FY 2012. As an integrated ERP system, LMP should have assumed the entire purchase requisition phase and eliminated the need for use of this legacy system. Depot personnel stated that they continued to use this system because LMP did not provide the resource managers with the ability to maintain proper funds certification and approval authority over purchase requests for services.

- ASA(FM&C) did not require AMC to reengineer the entitlement process and continued to require separate systems to entitle and disburse P2P transactions. Army managers informed us that during LMP development, DoD management instructed them not to reengineer the entitlement process because the replacement system for the Computerized Accounts Payable System and the Mechanization of Contract Administration Services system would subsume this functionality. However, in FY 2003, when DoD cancelled plans for the replacement system, ASA(FM&C) did not require AMC to reassess the requirements needed to integrate the entitlement process. Because Army managers did not reengineer the business process, they could not eliminate the prevalidation process designed to match proposed disbursements to actual obligations and eliminate unmatched disbursements.[3] By not reengineering the P2P business process, DoD must continue to operate and maintain stand-alone entitlement systems, such as the Computerized Accounts Payable System and the Mechanization of Contract Administration Services system, which LMP should have incorporated for AWCF activities. Integrating the entitlement process would also have eliminated the AWCF's portion of the more than 50 full-time equivalent DFAS positions charged to the Army by DFAS in FY 2010 to accomplish prevalidation and resolve unmatched disbursements.

The Army Director, OBT, issued the "Army Business Systems Information Technology Strategy," (Army ERP Strategy) on February 14, 2011. The Army ERP Strategy requires Army ERP program managers to assess current business operations and develop a plan to reengineer

[3] Prevalidation is the matching of an invoice and receiving report to the corresponding obligation recorded in LMP. It is required by public law and is a process that would be inherent in a fully integrated ERP environment because the same system performs the accounting and the entitlement functions.

the P2P business process.[4] Opportunities exist to integrate more functionality within LMP that would improve the control environment and make operations more efficient. For example, the Army ERP Strategy should detail how LMP personnel can configure the commercial software's functionality to perform the nonintegrated aspects of the P2P process, such as the contracting, commercial pay entitlement, and disbursement functions, to the maximum extent practical. In developing the Army ERP Strategy, Army managers should directly oversee all future development of LMP system requirements and develop a plan of action and milestones that will reengineer and integrate LMP to comply with the BEA P2P business process. This should include integrating to the maximum extent possible all phases of the P2P business process.

> *Opportunities exist to integrate more functionality within LMP that would improve the control environment and make operations more efficient.*

Implementing Control Activities to Accomplish Procure-to-Pay Business Process

Army managers did not establish the control activities needed to ensure that the P2P business process complied with financial reporting requirements. The Army had not correctly developed the following control activities to ensure proper implementation of the LMP P2P business process:

- top level functional and activity reviews of actual performance,
- performance measures and indicators, and
- proper execution of transactions and events.

Finding B addresses the control activities needed to assess segregation of duties and least privilege conflicts as well as restrict access to records and resources. Finding C addresses the need to provide Army ERP systems with accurate vendor master data.

Army Managers Not Performing Functional and Activity-Level Reviews of Actual Performance

Army managers did not conduct sufficient functional and activity-level reviews to assess the actual performance of the LMP P2P business process. Internal control standards require managers to compare actual performance to planned or expected results and conduct the analysis to correct significant differences. Although Army managers identified that abnormal account balances occurred in the eight accounts payable General Ledger Account Codes (GLACs) since the initial LMP deployment in FY 2003, they had not fully identified the reasons for the abnormal conditions. Consequently, they had not resolved this material weakness before full LMP deployment.[5] The 28 LMP activities reported more than $10.6 billion in abnormal

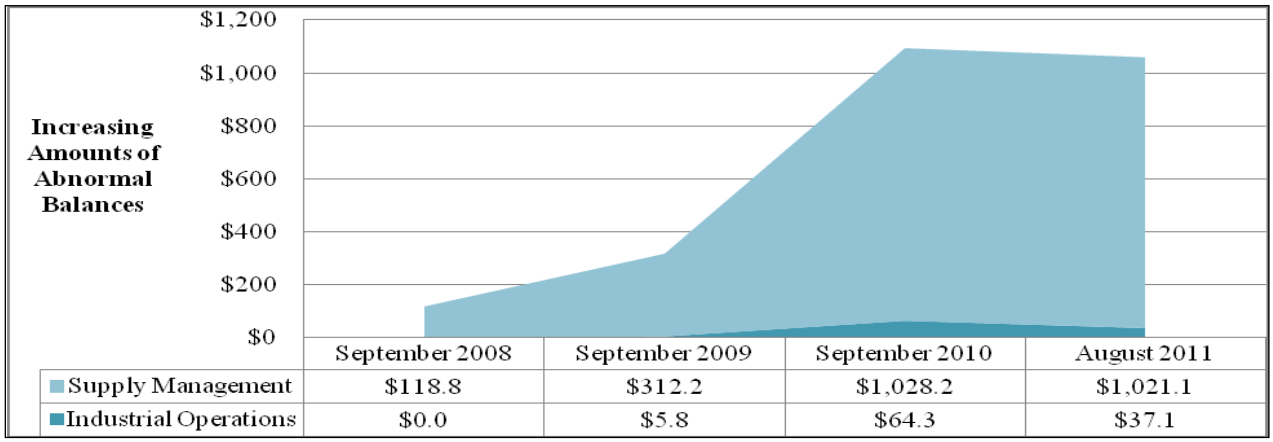
---

[4] The Army is also testing a pilot program within GFEBS to transition to an integrated entitlement process. We plan to assess the Army ERP Strategy as a separate audit.

[5] The 28 LMP activities report information in 14 general ledger accounts, 2 supporting accounts payable Federal and Non-Federal transactions, and 12 supporting budgetary information. Each account had several sub accounts that made up the value reported for the general ledger account. Each sub account had a designated normal debit or credit balance.

balances within 124 of 392 accounts payable and budgetary general ledger accounts that supported the P2P business process as of August 31, 2011. Figure 2 shows that the cumulative abnormal balances in the eight accounts payable general ledger sub accounts (GLAC 2110.XXXX) have significantly increased since September 2008 in the two AWCF business areas (Supply Management and Industrial Operations) as additional activities began using LMP.[6]

Figure 2. Abnormal Balances Reported in GLAC 2110
(millions)



	September 2008	September 2009	September 2010	August 2011
Supply Management	$118.8	$312.2	$1,028.2	$1,021.1
Industrial Operations	$0.0	$5.8	$64.3	$37.1

Source: LMP Trial Balance Data

The decision not to integrate the entitlement process into LMP was a significant reason for the abnormal balances in accounts payable. The lack of integration prevented LMP from recording the receipt and acceptance of goods before it recorded the payment transactions received from the disbursement system. LMP did not record the original accounts payable transaction at the time the Government actually accepted the goods at shipping points because the process sent the actual receipt documentation to the entitlement systems. Figure 3 shows the LMP accounting entry that should have occurred upon receipt of goods.

Figure 3. Accounting Entry to Post Goods Receipt Transaction

Debit - GLAC for specific asset or expense
Credit - Accounts Payable - Goods Receipt/Invoice Receipt, Federal/Non-Federal (GLAC 2110.1000/2000)

Source: Auditor Derived from SFIS Posting Logic

[6] Figure 2 uses the following general ledger sub accounts to make up Federal and Non-Federal Accounts Payable: Goods Receipt/Invoice Receipt Accounts Payable (Federal), GLAC 2110.1000; Goods Receipt/Invoice Receipt Accounts Payable (Non-Federal), GLAC 2110.2000; Accounts Payable – In-Transit, GLAC 2110.5000; Accounts Payable-Inventory Consignment Liability, GLAC 2100.6000; Accounts Payable (Federal), GLAC 2110.9100; and Account Payable (Non-Federal), GLAC 2100.9200. In FY 2011, the LMP Project Office added GLAC 2110.7100 and GLAC 2100.7200 to enable DFAS to enter a journal voucher at month end to create an accrual for constructive receipt of goods, which removes a portion of the abnormal balances.

When LMP received a disbursement transaction, the system posted an invoice receipt that moved the amount recorded as an accounts payable between accounts payable GLACs and then posted the actual disbursement to liquidate the accounts payable. Figure 4 shows the two accounting entries recorded when LMP posted disbursement transactions.

Figure 4. LMP Accounting Entries to Post Invoice and Disbursement Transactions

Debit - GLAC 2110.1000/2000 Credit - Accounts Payable - Federal/Non-Federal (GLAC 2110.9100/9200) Purpose: To post invoice receipt. Debit - GLAC 2110.9100/9200 Credit - Funds Balance With Treasury (GLAC 1010) Purpose: To post disbursement.

Source: Auditor Derived from LMP Posting Logic

The LMP posting logic for receipt of goods resulted in an abnormal debit balance in GLAC 2110.1000/2000. This abnormal balance remained until LMP personnel posted the actual receiving report, indicating receipt and acceptance of goods in LMP for the disbursement previously posted. Although Army managers and LMP Project Office personnel recognized this problem, they stated that commercial software would not allow them to record goods acceptance until after the goods actually arrived at a depot or supply management activity. They also stated that LMP could not use specific inventory movement codes that controlled in-transit inventory because the Army configured LMP to handle other inventory functions, which precluded the use of those codes.[7] They did not believe that commercial software developers would make the needed change to the software simply to support LMP. However, in March 2011, after we discussed with them the goods acceptance problem, the LMP Project Office requested a change to the commercial software and the company agreed to test a proposed solution in early FY 2012. If the Army had identified and corrected this system problem before full system deployment, ACWF abnormal accounts payable balances would not have grown to nearly $1.1 billion (Figure 2).

In addition, as of August 31, 2011, budgetary accounts supporting the P2P business process contained more than $9.5 billion in abnormal balances. The Army OBT and ASA(FM&C) should expedite the solution for resolving the posting of in-transit inventory. Once resolved, they should assess the system's business flow and posting logic for the accounts payable process and determine whether additional problems exist that cause abnormal balances related to the LMP P2P process. If additional problems exist, they should develop the corrective actions to address them.

---

[7] Inventory-in-transit is material in transit from commercial and government suppliers, whose title has passed to DoD, but has not been received and accepted at the final designated destination. Movement type 107 is used at the time of acceptance. This should create the necessary proprietary (GLACs 1510/2110) and budgetary (GLACs 4801/4901) postings. However, the accepted quantity will not be available for any logistical activity until an individual creates a Goods Receipt for the material using movement type 109. Movement type 109 will release the received quantity into unrestricted stock. This Goods Receipt transaction creates no financial postings.

Army Did Not Use Performance Measures and Indicators to Assessing Logistics Modernization Program System Performance

Army managers did not effectively use performance measures and indicators to assess the LMP data provided for their use. Internal control standards require that activities establish and monitor performance measures and indicators, including comparisons and functional reviews relating different sets of data to one another to make needed analyses of the relationships and develop appropriate corrective actions. Although Army managers had established some performance measures and indicators, they did not develop performance measures to monitor the status of the LMP Unobligated Authority for potential violations of the Antideficiency Act. Table 1 shows that the three LMP general ledger accounts used to report unobligated authority indicated the Supply Management activities had exceeded their cumulative unobligation authority by about $5.6 billion as of August 31, 2011. The table identifies the 11 Supply Management activities that had abnormal unobligated balances.

Table 1. Review of Unobligated Authority August 31, 2011
(millions)

LIMIT	Unapportioned Authority GLAC 4450	Allotments GLAC 4610	Commitments GLAC 4700	Total Unobligated Authority
AC50	$104.6	$0.0	$0.0	$104.6
AC5A	1,451.7	(126.6)	0.0	1,325.1
AC5D	474.0	(50.2)	(7.1)	416.7
AC5E	2,068.5	(42.7)	0.0	2,025.8
AC5F	189.1	(5.1)	(1.0)	183.1
AC5T	635.6	(14.8)	(5.2)	615.5
AC63	196.0	(6.9)	(26.8)	162.3
AC67	312.5	(1.2)	0.0	311.3
AC68	0.0	0.0	0.0	0.0
AC6E	(431.1)	(14.9)	(1.8)	(447.7)
AC9C	1,110.2	(15.2)	(150.8)	952.2
AC9D	573.7	448.0	(560.7)	461.0
AC9E	(244.3)	(59.5)	(49.4)	(353.2)
AC9F	(160.4)	(22.0)	(13.7)	(196.1
AC9G	16.6	(0.5)	0.0	16.0
Total	**$6,296.9**	**$88.4**	**$(816.7)**	**$5,568.6**

*The four-character limit represents the Supply Management activity and the shaded areas reflect an abnormal account balance. For example, AC50 represents the U.S. Army Materiel Command Logistical Operations. AC50 had an abnormal account balance of $104.6 million in both Unapportioned Authority (GLAC 4450) and Total Unobligated Authority.

Army Budget Office personnel stated that it was unlikely that the Supply Management activities had exceeded their obligation authority because they suspected that the LMP posting logic for three general ledger accounts, GLACs 4450, 4610, and 4700, was incorrect and caused LMP to report abnormal balances. They also stated that the abnormal balances reported in GLAC 4450

were incorrect balances brought forward from legacy systems that they planned to address once they fully identified and implemented the business process flows and accounting requirements for reporting contract authority within LMP. However, it was not until we questioned these accounts that Army managers took any actions to assess these abnormal accounts. Army Budget Office personnel did not believe an Antideficiency Act violation had occurred because their other reports showed sufficient balances in unobligated authority. However, LMP also indicated that the $448 million abnormal (debit) balance in GLAC 4610, "Allotments," at one activity (AC9D) resulted in the LMP trial balance reporting that the Supply Management business area exceeded its FY 2011 allotment authority by $88.4 million.

Army OBT and ASA(FM&C) should direct AMC financial managers to develop performance indicators to assist them in identifying activities exceeding their obligation or allotment authority. ASA(FM&C) should work with AMC to conduct a review of the LMP unobligated authority balances, determine whether a potential Antideficiency Act violation has occurred, and take actions to correct the LMP abnormal balances and posting logic problems. They should also develop a system edit check that identifies when an activity exceeds the allotment authority in GLAC 4610 and require activities to report each occurrence to the Office of ASA(FM&C) for immediate resolution.

Properly Executing Business Transactions and Events

LMP did not execute each phase of the P2P business process properly. The P2P business process required the assignment of specific accounting entries to record business transactions to the GLACs. As stated in DoD IG Report No. D-2011-015, Army managers could not provide the detailed posting logic used for each financial event. Without this information, Army managers had limited assurance that LMP could properly execute P2P transactions and events. Internal control standards state that proper documentation of posting logic is essential to ensuring that the proper execution of transactions occurred. Both AWCF activities reviewed had problems with the execution of the business transactions and events related to the Requisitioning and Commitments Phase and the Contracting and Obligations Phase of the LMP P2P business process. Without automated system controls, unauthorized persons could submit or change transactions and accomplish business events outside the scope of their authority. As a result, data from LMP are subjected to an increased vulnerability for individuals to create and process fraudulent transactions. Instituting automated system controls is the principal means of ensuring that the Army only initiates or enters valid transactions.

Logistics Modernization Program System Did Not Implement the Requisitioning and Commitments Phase Effectively

Army managers did not sufficiently assess the Requisitioning and Commitments Phase at AWCF activities and design the LMP functionality needed to create and process all requisitions and commitments used by AWCF activities. This phase requires an individual to create a purchase request (requisition) and establish a commitment of funds to record in the accounting records. At the two AWCF activities we visited:

- LMP did not have the proper functionality to create purchase requests related to service contracts and credit card transactions. Instead, activity personnel continued to use offline

systems and processes to create purchase requests and entered a manual commitment transaction within LMP to track the purchase request using the LMP transaction screen FMY1 (Create Funds Commitment).

- LMP did not restrict purchase request functions, such as purchase request approvals, document releases, and waiving ordering limits, to only those high-level managers required to perform the actions. For example, LCMC users performed a manual process to obtain higher management approvals for purchase requests because LMP did not automatically route purchase requests to high-level managers for approval. Army managers also did not implement the system controls needed to restrict the release of purchase requests to the proper approval authority.

- More than 1,300 of the 3,514 users had system access that permitted them to create, change, and release a purchase request for any dollar amount without approval from a higher level of authority. Internal control standards state that the individual requesting items should not also approve that request. LMP needs to be able to provide the ability to track approval events online by transaction and approval level, including the date, time, and signature of the approving authority (see Finding B).

- LMP lacked the system controls to route purchase requests to resource management personnel to formally record fund certification. The BEA business rules required the certification of funds availability by the comptroller or an individual responsible for the funds to ensure obligations would not exceed available funds. LMP allowed any individual with authority to create a purchase request to fund the request based on entering a code other than "U" in the Account Assignment Category before releasing the document to the contracting office. Personnel at the two activities stated that individuals releasing purchase requests could also cite other activities' funds unintentionally. The Depot provided a recent example of Corpus Christi Army Depot citing the Depot's funds by incorrectly entering the wrong Plant Number into LMP. As a result, Corpus Christi Army Depot erroneously committed $8,253 in Depot funds. The Depot and Corpus Christi Army Depot worked together to correct the error.

To ensure proper funds control, only the individual responsible for the obligation authority provided to an AWCF activity, or a limited number of individuals appointed by that individual to certify funds, should be able to fund purchase requests. This certification requires the use of an electronic signature that controls the certified document and provides the contracting officer or obligating official the legal authority to use the funding.

In addition, the two AWCF activities visited committed funds at different points during the phase. For example, the Depot committed funding upon release of the purchase request for obligation actions and the LCMC did not commit funding until notified by the contracting office that a contract was ready for obligation actions. LMP users at the LCMC continued to follow the legacy policy and prepared unfunded purchase requests. AMC managers stated that this occurred in order to prioritize the use of funds because many of the procurements had long administrative lead times. DoD Financial Management Regulation 7000.14-R (DoD FMR), volume 14, chapter 1, "Administrative Control of Funds," January 2009, requires that proper

funding be available prior to initiating contracting or other obligation actions. Therefore, personnel should commit funds at the time they release purchase requests for action by others. By not committing the funds upon release of a purchase request, DoD is at risk of accomplishing costly contracting actions and not having funds available to obligate the contract at the time of award.

The Army OBT and ASA(FM&C) should direct AMC to develop the functionality to provide for proper document flow for approval of purchase requests within LMP. They should also direct AMC to evaluate the P2P business process to identify all offline systems and procedures that activities use to accomplish the Requisitioning and Commitments Phase outside of the ERP system and, to the extent possible, incorporate that functionality into LMP and discontinue the use of the other processes. In situations where Army managers cannot immediately incorporate the functionality into LMP, they should develop compensating controls over non-integrated offline processes and restrict the creation of manual commitment transactions to resource management personnel. They should also restrict an individual's ability to use fund codes and approve transactions to only the individual's LMP activity. The Army OBT and ASA(FM&C) should also direct AMC to assign funds certification authority to a limited number of individuals and develop the requirement for LMP to limit funds certification to only these individuals. In addition, they should direct that fund managers establish commitments for purchase requests at the time of release.

Limited Reengineering of the Contracting and Obligations Phase

Army managers did not sufficiently reengineer the Contracting and Obligations Phase of the P2P business process to ensure that LMP controlled obligation transactions without the need for locally developed manual processes. Army managers relied on interfaces they developed with existing contracting systems such as the Standard Procurement System and Procurement Automated Data and Document System to develop the obligations based on the contracting actions those systems accomplished. However, LMP did not provide the online capability for individuals to accomplish Military Interdepartmental Purchase Request (MIPR) acceptance functions. Instead, the requesting activity had to print and manually sign a hardcopy MIPR document and send it to the performing activity. The performing activity manually accepted the MIPR and sent it back to the requesting activity. LMP then allowed the individual who created the MIPR at the requesting activity to record the actual acceptance by the performing activity and establish the obligation. This partially automated process provided only limited control over the obligation process and is prone to error. The use of manual processes prevented the Army managers from realizing the integration advantages LMP could have provided by systematically controlling the MIPR request and acceptance process.

> *. . . LMP did not provide the online capability for individuals to accomplish Military Interdepartmental Purchase Request (MIPR) acceptance functions.*

In addition, the LMP Program Activity Table used by the requesting activity contained invalid address information for the performing activities and did not generate an accurate hardcopy MIPR for mailing purposes. LCMC personnel showed us that the LMP Program Activity Table was incomplete and required them to prepare a manual MIPR document for submission to the receiving activity for acceptance. The Army OBT and ASA(FM&C) should direct AMC to

evaluate the P2P business process to identify the offline systems and procedures within the Contracting and Obligations Phase, develop plans for incorporating these functions and integrating the acceptance functionality into LMP, and discontinue the use of manual obligation processes once the integration into LMP is complete. In addition, they should direct AMC to ensure that the data contained in the Program Activity Table can be used to prepare manual documents correctly and develop compensating controls to validate the data integrity of manually created obligation transactions.

Goods Receipt and Invoicing Phases Not Properly Reengineered

Army managers did not reengineer the AWCF business process to correctly record accounting transactions within the Goods Receipt and Invoicing Phases. The Army decided to continue using legacy entitlement systems to accomplish these phases instead of incorporating them into LMP. Consequently, Army managers did not design LMP to receive invoices directly from contractors and vendors or receiving reports from activities authorized to accept goods on behalf of the government. Instead, the Wide Area Workflow system only provided these automated documents to the entitlement systems, which eventually provided LMP with payment transactions. When DoD receiving activities accepted supply items at the shipping point, the Army delayed the recording of the receipt and acceptance data in LMP until these items actually arrived at the receiving dock. In these situations, LMP did not record the associated accounting transactions for government acceptance of goods correctly because AMC personnel developed incorrect posting logic to record these transactions.

The LMP process contributed to the creation of abnormal balances in the accounts payable and associated general ledger accounts. For example, when LMP received a payment transaction from an entitlement system before properly recording the government receipt and acceptance of the goods, it erroneously treated these transactions as if they were a prepayment of an undelivered order. LMP recorded the transaction by crediting "Undelivered Orders-Paid" (GLAC 4802) in the budgetary accounts, but incorrectly debited GLAC 2110 in the proprietary account instead of "Advances and Prepayments" (GLAC 1410) to reflect payment of a prepaid undelivered order. This created abnormal account relationships and abnormal balances in the accounts. LMP should have posted the receipt and acceptance of the goods since the entitlement system had already properly matched the obligations to a valid invoice and receiving report using the prevalidation process.

Beginning in April 2011, the Army approved a departmental-level journal voucher that posts the correct LMP accounts and serves as a temporary fix until the Army managers can implement the software changes needed to record in-transit inventory movements correctly. The posting logic discussion on pages 9 and 10 explains the significance of LMP not recording the receiving data at the time of acceptance.

Although LMP could identify the transactions that comprised the unadjusted trial balance and the information we obtained from DFAS personnel supported an audit trail, LMP did not accurately record the source documentation information for transactions recorded during the Goods Receipt and Invoicing Phases. Internal control standards require the accurate recording of transactions to maintain their relevance and value to management in controlling operations and making decisions. We selected a random stratified sample of 120 P2P transactions recorded as

"Delivered Orders-Obligations Paid" (GLAC 4902) made during November 2010 and attempted to track the information recorded in LMP to the source documents that activities and vendors had provided to the entitlement systems. We were able to trace the dollar value of the transactions recorded in GLAC 4902 from the unadjusted trial balances of each of the 29 LMP activities to the total dollar value of disbursement transactions recorded in LMP. For each of the randomly selected P2P transactions, based on the document voucher number found in LMP, we requested the voucher, vendor invoice, and receiving report from DFAS Columbus. DFAS Columbus personnel provided supporting documents for 96 of the 120 transactions.[8] Supporting documents for the 96 transactions presented the following deficiencies:

- LMP did not record the actual invoice number from the vendor. The Core Financial System Requirements state that systems must provide automated functionality to capture invoice data, including the vendor invoice number.

- LMP did not correctly record invoice dates, invoice receipt dates, receipt dates, or acceptance dates as reflected on the source documents. The dates recorded in LMP usually reflected the dates LMP interfaced with the entitlement system.

- The pertinent LMP invoice and receiving report transaction screens did not identify the disbursement voucher information. Because more than one disbursement typically liquidated an obligation, LMP needed to link the various invoices and receiving reports to the corresponding disbursement voucher.

The absence of actual invoice numbers, accurate dates, and disbursement voucher information prevented activities from using LMP to detect duplicate payments and validate that payments complied with the Prompt Payment Act. In addition, the incorrect data did not allow us to evaluate the validity of the data LMP used to approve prevalidation requests. LMP did not have a standard query to identify all the documents related to a P2P transaction. The Core Financial System Requirements state that systems must provide the capability to perform a query that would list all related documents and transactions in the processing chain for document referencing and audit trail purposes. The Army OBT and ASA(FM&C) should direct AMC to develop functionality in LMP to capture and record the vendor invoice date, vendor invoice number, and date of invoice receipt at the paying station. Army managers should direct the LMP Project Office to develop the data fields needed to record the actual receipt and acceptance dates for goods and services and a query that will identify all documents related to an LMP P2P transaction.

The absence of actual invoice numbers, accurate dates, and disbursement voucher information prevented activities from using LMP to detect duplicate payments and validate that payments complied with the Prompt Payment Act.

[8] The remaining 24 transactions represented inter-AWCF transactions and material movements. It appeared proper for activities to record the types of transactions in this account. However, because there were no source documents, such as disbursement vouchers, vendor invoices, or receiving reports, we excluded them for our review.

Army Managers Did Not Integrate Entitlement and Disbursement Phases

LMP did not use the commercial software functionality for entitling and disbursing P2P transactions because Army managers used legacy entitlement and disbursement processes to perform the ready-to-pay functions using the Wide Area Workflow system and existing entitlement systems. They informed us that they would continue to use those processes until DoD decided how to replace the legacy entitlement systems. As a result, the Army and DFAS had to develop interfaces within LMP to prevalidate commercial payments. The entitlement process integration would have eliminated the need for a separate prevalidation system and would reduce the need for some of the 50 full-time equivalent DFAS positions and prevalidating, disbursing, and resolving unmatched disbursement for the Army in FY 2010.

Prevalidation processing in LMP did not result in the recording of the proper accounts payable and ready-to-pay transactions.[9] Although LMP recorded the invoice and the required budgetary accounting entry upon receiving a prevalidation request, it did not determine whether the LMP activity had previously recorded a receiving report and the associated accounts payable transaction. LMP Project Office personnel stated that LMP tracked prevalidation requests using the Authorization Reference Number provided by the prevalidation module, but LMP did not record the approval of these prevalidation requests as "Disbursements In-transit" (GLAC 2120) to recognize that LMP had approved the account payable transaction for payment. As a result, LMP did not create the ready-to-pay transaction file required by the U.S. Government Standard General Ledger to reconcile to the disbursement transaction file once received. ASA(FM&C) should develop a plan to implement the functionality in LMP to record the receipt and acceptance of goods and services, receipt of the invoice requesting payment, and allow LMP to perform the appropriate obligation matches as required by the Core Financial System Requirements.

Because disbursement transaction files did not identify the prevalidation requests approved for disbursement by Authorization Reference Number, LMP could not reconcile the transactions and had difficulty posting disbursement transactions to matching detailed obligations, creating unmatched disbursements. Examination of the more than 83,000 disbursements made in November 2010, determined that LMP posted unmatched disbursements for 8,244 transactions, valued at about $339.5 million. A duplicate obligation ("ZK" transaction) was created for each unmatched disbursement transaction it received.[10]

LMP automatically created a "ZK" transaction without accounting office personnel first performing the research required by DoD FMR, volume 3, chapter 11, "Unmatched Disbursements, Negative Unliquidated Obligations, and In Transit Disbursements," November 2010, to determine whether a matching obligation existed. The creation of each "ZK" transaction required LMP users to record at least two additional LMP transactions once they

---

[9] Ready-to-pay means that the proper three-way match between the obligation, invoice, and receipt occurred and an individual certified the payment as ready for transmission to a payment office for action.

[10] A "ZK" transaction is a potential duplicative obligation established in LMP that matches disbursement received from a payment office for which a matching obligation can be readily identified. The "ZK" transaction remains in LMP until manual research identifies the original obligation.

identified the correct obligation, one transaction to reverse the "ZK" transaction and another to post the disbursement to the correct obligation. LMP erroneously recorded the unmatched disbursement transactions as a contract expense and cited funds from the associated LMP activities' allotment account (GLAC 4610) for these pseudo obligations. The LMP activities reversed the pseudo obligations once they identified the matching obligations, which took from 1 day to more than 1 year. An obligation previously existed in LMP for each of the 43 randomly selected unmatched disbursement transactions recorded in the November 2010 disbursement file we selected for review. Dual posting of obligations reduced the availability of funds and could cause the Army to exceed its annual obligation authority and incur a potential violation of the Antideficiency Act.

LMP erroneously recorded the unmatched disbursement transactions as a contract expense and cited funds from the associated LMP activities' allotment account (GLAC 4610) for these pseudo obligations.

As discussed previously, LMP contained no system controls or edit checks that would alert Army managers when LMP activities attempt to process transactions that will cause the over expenditure of their allotted obligation authority. ASA(FM&C) should direct AMC G-8 to develop the requirements in LMP to create a ready-to-pay file based on the LMP approval of prevalidation requests. ASA(FM&C) and AMC personnel should stop allowing LMP to create a temporary obligation automatically for each disbursement it cannot match to a detailed obligation. LMP should record these transactions as unmatched disbursements and ASA(FM&C) should require accounting activities to perform the research required to determine whether they can identify the correct detailed obligation. If one exists, they should post the disbursement to that obligation and, if not, they should take immediate actions to record the obligation.

Ineffective Monitoring of the Army Procure-to-Pay Business Process

Army managers did not ensure that LMP activities and AMC managers monitored operations within the LMP P2P process. AMC managers did not revise quality assurance evaluations used in the legacy environment to assess controls implemented in the ERP environment. Evaluations of internal controls performed at the two activities relied on checklists developed before the implementation of LMP. Consequently, these activity personnel did not adequately assess the LMP system controls and the manual P2P processes that the activities performed. In FY 2010, the activities had performed some reviews that identified abnormal balances existed in their general ledger accounts. However, the Army's departmental-level financial reporting processes masked the abnormal account balances by netting the account balances of all the AWCF activities and reported normal account balances on the AWCF financial statements. This precluded senior Army resource and financial managers from properly gauging the results of normal LMP business operations.

Headquarters AMC had not determined the internal control procedures and checklists needed to assess any of the LMP processes. During the audit, AMC managers established a working group to begin establishing the framework for a more robust internal control assessment of the LMP

P2P business processes. ASA(FM&C) should direct AMC to develop a comprehensive internal control program to assess the quality of LMP performance and regular management and supervisory activities over the LMP P2P business process.

Conclusion

Army managers did not perform sufficient business process reengineering to implement the BEA's P2P business process within LMP successfully. Instead, the Army recreated most of the legacy business processes within LMP, which did not correct the long-standing material weaknesses within the P2P business process. Army managers did not assess all offline systems and procedures used by the LMP activities to create, approve, and reconcile P2P transactions and design the LMP functionality needed to accomplish those tasks. As of August 31, 2011, LMP Project Office and AMC activities created numerous workarounds that resulted in LMP implementing incorrect posting logic that resulted in abnormal balances and account relationships of $10.6 billion. Army managers did not develop performance measures to assess LMP data and implement the corrective actions needed to resolve known problems.

Dual processing and posting of contract data, receiving reports, and invoices in both an entitlement system and LMP was inefficient, prone to errors, and obscured the audit trail back to source documents and transactions. The lack of integrated LMP business processes required the Army and DFAS to continue performing costly prevalidations to ensure proper obligation matching required by the Core Financial System Requirements and reconciliations to maintain the correct data between the systems. In addition, Army managers did not ensure that LMP activities and AMC managers monitored operations within the LMP P2P business process. As part of the new Army ERP Strategy, the Director, Army OBT and ASA(FM&C) should develop a plan of action and milestones to bring the LMP system into compliance with BEA P2P business rules. The ASA(FM&C) should work with AMC G-8 to conduct a review of the LMP unobligated authority and determine whether an Antideficiency Act violation occurred when LMP activities appeared to exceed their AMC allotted authority. They also should redesign the LMP prevalidation process, stop automatically establishing obligations for unmatched disbursements until activities accomplish proper reconciliation as required by the DoD FMR, and develop a system edit check that identifies when an activity exceeds the allotment contained in GLAC 4610. In addition, ASA(FM&C) should direct the AMC internal control managers to develop a comprehensive internal control program to assess the LMP P2P business process.

Recommendations, Management Comments, and Our Response

A.1. We recommend that the Director, Army Office of Business Transformation and Assistant Secretary of the Army (Financial Management and Comptroller) develop a plan of action and milestones to bring the Logistics Modernization Program system into compliance with the DoD Business Enterprise Architecture Procure-to-Pay business rules. Specifically, as part of the Army Business System Information Technology Strategy, define the Army's plans for developing effective and efficient Logistics Modernization Program system business processes that will:

a. Integrate the contracting and entitlement functions.

Department of the Army Comments

The ASA(FM&C), responding on behalf of the Army, agreed and stated that Army managers recognize that opportunities exist to improve the efficiency of the LMP P2P processes. The ASA(FM&C) stated that current process segmentation adds to interface complexity and error rates and is a source of abnormal balances. The ASA(FM&C) also stated that the LMP system design is normal for typical ERP implementation and the best practice is to reduce risk associated with large implementation projects by first fielding a basic capability and then capitalizing on investment via driving more functionality into the system. As part of the Army Business System Information Technology Strategy, Army managers will review the feasibility of integrating additional P2P functionality within the LMP environment and will use the results of the review to develop a plan of action and milestones addressing the viability of integrating additional contracting and entitling functions, improving internal controls, and identifying additional metrics and performance indicators. The plan of action and milestones will reflect limitations imposed by the Department's BEA related to contract writing, vendor invoicing, payment entitlements, and disbursement processing.

Our Response

The Army comments were partially responsive. In the Army plan of action and milestones, Army managers should address how to reengineer the Army current business processes to remove or mitigate any limitations the Army believes are imposed by the BEA requirements and then work with DoD senior leadership to implement the reengineered business processes. We request that the ASA(FM&C) provide additional comments on the final report, explaining how the Army will implement the reengineered business processes.

b. Expedite a solution for resolving the in-transit inventory posting logic problems and correct abnormal balances.

Department of the Army Comments

The ASA(FM&C), responding on behalf of the Army, agreed and stated that the December 2011 software release added capabilities for constructive receipts, automated in-transit inventory accrual processes, improved the derivation of the trading partner indicator, corrected posting logic resulting in the reduction of abnormal balances, and improved access controls to prevent inaccurate cross-command postings. The ASA(FM&C) reported that these improvements resulted in a $1.9 billion reduction in abnormal balances between August 2011 and December 2011.

Our Response

The Army comments were responsive.

c. Reassess the system's accounts payable business process flow and posting logic and determine whether additional problems exist that cause abnormal balances. If so, develop the corrective actions needed to resolve those problems.

Department of the Army Comments

The ASA(FM&C), responding on behalf of the Army, agreed and stated that the feasibility review and P2P plan of action and milestones will identify additional opportunities to enhance LMP P2P processing. The ASA(FM&C) stated that Army managers made significant changes during 2011 that corrected the current configuration of transactions for contract authority, corrected posting logic for credit card expenses, and enhanced configuration of Defense Travel System and Integrated Product-Support Vendor transactions. Additionally, the December 2011 software release added capabilities for constructive receipts, automated in-transit inventory accrual processes, and improved the derivation of trading partner indicator information. The ASA(FM&C) also stated that the corrected posting logic resulted in the reduction of abnormal balances and improved access controls to prevent inaccurate cross-command postings.

Our Response

The Army comments were responsive.

d. Develop performance indicators to assist in identifying the potential for significant posting errors and develop responsive corrective actions.

Department of the Army Comments

The ASA(FM&C), responding on behalf of the Army, agreed and stated that the Army will perform a feasibility review as part of the Army Business System Information Technology Strategy and use the results to develop a plan of action and milestones addressing additional metrics and performance indicators.

Our Response

The Army comments were responsive.

e. Develop the edit checks and business workflows needed to control and route purchase requests and Military Interdepartmental Purchase Requests to the appropriate individuals for approval and funds certification. This should include:

(1) Associating fund codes and approval authority to an individual's assigned activity.

(2) Assigning certification of funds availability to a limited number of individuals and developing the requirement for the system to limit funds certification to only these individuals.

(3) Directing that fund managers establish commitments for purchase requests at the time an activity releases the requests for obligation actions.

(4) Developing the functionality needed for separate individuals to create and accept Military Interdepartmental Purchase Requests within the system.

(5) Validating the data contained in the Program Activity Table and ensuring that it is preparing manual documents correctly and developing compensating controls to validate the data integrity of manually created obligations.

Department of the Army Comments

The ASA(FM&C), responding on behalf of the Army, agreed and stated that the Army will continue to leverage the Army Business System Information Technology Strategy and governance procedures to implement additional improvements as updates to the BEA and SFIS are published. The ASA(FM&C) stated that the Army is in requirements definition discussions for Local Vendor Pay enhancements that will enable LMP to perform entitlement functions currently processed by other systems. These requirements include edit checks and business workflows needed to control and route purchase requests and MIPRs through LMP to the appropriate individuals for approval and funds certification, management of vendor data, and entitlement functions. The Army expects to complete a requirements analysis by March 2012.

Our Response

The Army comments were partially responsive. Although the ASA(FM&C) stated that the Army will define requirements for the Local Vendor Pay enhancements, she did not specifically state how her office will ensure that the enhancements will address the specific issues identified in the recommendation. We request that the ASA(FM&C) provide additional comments on the final report, explaining how the enhancements will resolve the deficiencies in processing purchase requests and MIPRs.

f. Identify offline systems and procedures within the Procure-to-Pay phases, incorporate the functionality into the system, and discontinue the use of offline processes. In situations where Army managers cannot immediately incorporate the functionality, develop compensating controls over non-integrated offline processes and restrict the creation of manual commitment and obligation transactions to resource management personnel.

Department of the Army Comments

The ASA(FM&C), responding on behalf of the Army, agreed and stated that the Army will continue to leverage the Army Business System Information Technology Strategy and will review the feasibility of integrating additional P2P functionality into LMP. The results of the review will be used to develop a plan of action and milestones addressing the viability of integrating additional contracting and entitling functions, improving internal controls, identifying and correcting abnormal balances relating to P2P transactions, and developing and tracking requirements imposed by the Department's BEA related to contract writing, vendor invoicing, payment entitlements, and disbursement processing.

Our Response

The Army comments were partially responsive. Although the ASA(FM&C) stated that the Army will develop a plan of action and milestones, she did not state that the Army will develop compensating controls for nonintegrated offline processes and restrict the creation of manual commitment and obligation transactions to resource management personnel. We request that the

ASA(FM&C) provide additional comments on the final report, explaining how the Army will ensure that proper compensating controls are developed until related functionality is incorporated into LMP.

g. Develop functionality within the system to capture and record the actual vendor invoice date, vendor invoice number, and date of invoice receipt at the paying station. Also, develop the data fields needed to record separately the actual receipt and acceptance dates for goods and services.

Department of the Army Comments

The ASA(FM&C), responding on behalf of the Army, agreed and stated that the plan of action and milestones will reflect limitations imposed by the Department's BEA related to contract writing, vendor invoicing, payment entitlements, and disbursement processing. The ASA(FM&C) also stated that Army managers are currently in requirements definition discussions for Local Vendor Pay enhancements, which would enable LMP to perform vendor payment functions.

Our Response

The Army comments were partially responsive. The ASA(FM&C) did not identify how the Army will develop functionality within LMP to capture and record the actual vendor invoice date, vendor invoice number, and date of invoice receipt at the paying station. Also, the ASA(FM&C) did not identify how the Army will develop the data fields needed to record separately the actual receipt and acceptance dates for goods and services. Dual processing and posting of contract data, receiving reports, and invoices in both an entitlement system and LMP was inefficient, prone to errors, and obscured the audit trail back to source documents and transactions. We request that the ASA(FM&C) reconsider her response to this recommendation and provide additional comments on final report, addressing how LMP will capture the appropriate invoice and receiving data needed to support obligation matching and prompt payment requirements.

h. Develop the ability to identify all documents related to Procure-to-Pay transactions within a single system query.

Department of the Army Comments

The ASA(FM&C), responding on behalf of the Army, agreed and stated that as part of the Army Business System Information Technology Strategy, the Army will review the feasibility of integrating additional P2P functionality within the LMP environment. The results of the review will be used to develop the plan of action and milestones.

Our Response

The Army comments were partially responsive. The ASA(FM&C) identified the need to develop a plan of action and milestones to address this recommendation. However, she did not address how or when the Army will address implementing LMP functionality to identify all documents related to the P2P transactions using a single query. The Core Financial System Requirements state that systems must provide the capability to perform a query that would list all

related documents and transactions in the processing chain for document referencing and audit trail purposes. The absence of actual invoice numbers, P2P processing dates, and disbursement voucher information prevented activities from using LMP to detect duplicate payments and validate that payments complied with the Prompt Payment Act. We request that the ASA(FM&C) reconsider her response to this recommendation and provide additional comments on the final report, addressing how the Army will implement this query function within LMP.

i. Develop a ready-to-pay file based on the system's approval of prevalidation requests.

Department of the Army Comments

The ASA(FM&C), responding on behalf of the Army, agreed and stated that as part of the Army Business System Information Technology Strategy, the Army will review the feasibility of integrating additional P2P functionality within the LMP environment. The results of the review will be used to develop the plan of action and milestones.

Our Response

The Army comments were partially responsive. The ASA(FM&C) identified the need to develop a plan of action and milestones to address this recommendation. However, the ASA(FM&C) did not specifically address the Army's plan for developing LMP processes that will create a ready-to-pay file based either on an approved prevalidation request or invoices approved through the integrated entitlement function being developed in LMP. Implementing the functionality in LMP to record the receipt and acceptance of goods and services and the receipt of the invoice requesting payment will allow LMP to perform the appropriate obligation matches as required by the Core Financial System Requirements. The Disbursements In-Transit general ledger account (GLAC 2120) should liquidate an existing accounts payable transaction based on the certification and transmission to a disbursing activity of that invoice for payment. GLAC 2120 should be liquidated upon the posting of a related disbursement transaction returned by the disbursing station. We request that the ASA(FM&C) reconsider her response to this recommendation and provide additional comments on the final report, explaining how the Army will develop the required LMP functionality.

A.2. We recommend that the Assistant Secretary of the Army (Financial Management and Comptroller) direct the Army Materiel Command G-8 to:

a. Conduct a review of the unobligated authority general ledger account balances to determine whether an Antideficiency Act violation occurred, and take actions to correct the abnormal balances and posting logic problems related to the accounts.

b. Modify the Logistics Modernization Program system to cease the automatic obligation of unmatched disbursements until activities accomplish proper reconciliation as required by the DoD Financial Management Regulation.

c. Develop a system edit check that identifies when an activity exceeds the allotment contained in General Ledger Account Code 4610 and require activities to report each

occurrence to the Office of Assistant Secretary of the Army (Financial Management and Comptroller) for immediate resolution.

Department of the Army Comments

The ASA(FM&C) agreed and stated that she will direct Headquarters AMC to work with DFAS Columbus to review the unobligated authority general ledger accounts balances for all LMP activities and determine if any have exceeded their obligation authority. If this review discloses the potential for an Antideficiency Act violation, appropriate action will be taken. Abnormal balances disclosed by the review will be corrected. The Army will complete the review by June 2012. In addition, the Army conducted a workshop in March 2012 to determine a compliant LMP process and discontinue the automatic obligation process for unmatched disbursements. The ASA(FM&C) also stated that the Army will use existing reports to better monitor and flag potential issues with GLAC 4610, "Allotments." The Army will include milestones related to these actions in the P2P plan of action and milestones developed in response to Recommendation A.1.

Our Response

The Army comments were responsive.

A.3. We recommend that the Assistant Secretary of the Army (Financial Management and Comptroller) direct the development of a comprehensive internal control program for the Logistics Modernization Program Procure-to-Pay business process to assess the quality of performance and regular management and supervisory activities over the business process. Army managers should work with Logistics Modernization Program Project Office personnel to ensure that they design and implement the necessary procedures and controls and develop the testing needed to ensure control effectiveness.

Department of the Army Comments

The ASA(FM&C) agreed and stated that the Army will assess key controls supporting all Financial Improvement and Audit Readiness assessable units, including those related to P2P activities, as part of the Army Financial Improvement Plan audit readiness discovery and evaluation activities. The assessment will determine the effectiveness of the design and operation of applicable controls and identify corrective actions required to bring controls into compliance with audit standards. The ASA(FM&C) also stated that the assessment might also recommend establishing a standard performance objective for those managers and supervisors working P2P processes. These actions will be completed during FY 2013.

Our Response

The Army comments were responsive.

Finding B. Logistics Modernization Program System Access Controls Were Ineffective

Army managers did not establish LMP Functional Security Roles (FSRs) and other system access procedures to ensure proper data integrity of the P2P business process. This occurred because they did not provide effective oversight over the development and implementation of the LMP FSR templates. Specifically, Army managers did not:

- develop a risk matrix that alerts managers of potential segregation of duties and least privilege conflicts caused by assigning multiple LMP transaction screens within FSR templates,
- develop adequate policies and procedures to ensure that system administrators and user supervisors effectively administered user access, and
- perform periodic reviews of LMP user access.

As a result, the two activities we visited assigned 624 users FSRs that would cause segregation of duties conflicts. In addition, users had more access than required and were granted access to perform functions without proper authorizations. Further, LMP User Account Management (UAM) administrators had not resolved or removed over 7,000 suspended user accounts. The administration of user access placed LMP data at an increased risk for unauthorized and fraudulent use.

System Compliance with Federal Information Security Management Act

Public Law 107-347, "E-Government Act of 2002," December 17, 2002, Title III, enacted Federal Information Security Management Act (FISMA) of 2002 and required each Federal agency to develop, document, and implement an agency-wide program that provides security for the information and systems supporting that agency's operations and assets. FISMA required that the National Institute of Standards and Technology (NIST) develop and issue standards, guidelines, and other publications to assist Federal agencies in implementing and managing cost-effective programs to protect their information system data. NIST Special Publication 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations," May 2010, addressed specific requirements for implementing proper separation of duties, least privilege, and account management. [11] See Glossary for a definition of these terms. The NIST requirements related to segregation of duties, least privilege access, and account management provide the indicators of how well LMP safeguarded data integrity.

Role-Based Access Control Model

NIST Information Technology Laboratory Bulletin, "An Introduction to Role-Based Access Control," December 1995, defined guidance for developing a role-based access control model.

---

[11] Internal control standards issued by the GAO refer to segregation of duties. NIST publications refer to separation of duties instead of segregation of duties. Within the report, we use segregation of duties.

The model required Army managers to perform a thorough analysis of how an entity operated and how users functioned within an entity. The model also allowed access control policies to align with the organizational lines of authority and responsibilities of the individual users. The model provided an effective means for developing and enforcing LMP specific security polices, including segregation of duties and least privilege, and for streamlining the account management process. FSR templates identify the access and authorizations granted to a user and are associated with the user profiles in the commercial software. When designed properly, each FSR template should contain the minimum set of privileges required to perform assigned tasks or functions.

Developing Logistics Modernization Program Functional Security Role Templates

As of August 4, 2011, the LMP Project Office had developed 376 FSR templates to assign LMP user access. Each template incorporates the applicable transaction screens needed to perform standard LMP functions.[12] For example, FSR template "R/3 ACQ Change Purchase Requisition NB ZB" provides the ability to modify a purchase request using the ME52N transaction screen. The template also allows users to view any LMP purchase request using the ME53N transaction screen. See Appendix F, Table F-1 for titles of transaction screens. The LMP Project Office worked with the UAM managers from each LMP activity to tailor the FSR templates to the functions performed within each AWCF activity.

Issuance of Army Materiel Command User Access Policy

During 2007, AMC, G-3, issued the LMP End User Access and Account Management Policy (LMP User Access Policy), which designated the Enterprise Integration Directorate as the overall policy administrator for LMP user access and account management. The policy assigned the commander at each LMP activity the responsibility to appoint an UAM manager to oversee and manage the activity's LMP system access.

Segregation of Duties and Least Privilege Controls

Army managers did not establish the proper data integrity controls to resolve segregation of duties and least privilege conflicts when they provided the requirements the LMP Project Office used to develop the LMP FSR templates.[13] The LMP Project Office used the role-based access model for developing the FSR templates and designed the FSR templates to accomplish the specific job functions as defined by AMC managers. It had also designed specific FSR templates as "Restricted" to allow activities to limit access to certain transaction screens to only those users needing to accomplish a specific task for limited periods. For example, the LMP Project Office created restricted FSR templates that limited the ability of users to modify the LMP vendor master information or approve certain transactions, such as employee timesheet data. Restricted

---

[12] Each function may have one or more LMP transaction screens associated with it. Each transaction screen may require the access for one or more authorization fields and was identified by a unique code consisting of letters and numbers.

[13] Least privilege requires that activities assign user access based upon the minimum access that a user requires when performing the tasks assigned by business function and organization.

FSR templates required an additional level of approval from the Business Transformation Lead responsible for that business process at each LMP activity. However, Army managers did not adequately map each of the individual FSRs they created to the P2P business process. Consequently, they had limited assurance that segregation of duties or least privilege conflicts would not occur when they created individual FSR templates or when authorized individuals at AWCF activities assigned multiple FSRs to users.

Assessing Templates for Procure-to-Pay Business Process Conflicts

Army managers did not determine which transaction screens, when assigned together, caused segregation of duties conflicts. At least 82 of the 302 FSR templates had a direct relationship to the P2P business process and 13 of the 82 FSR templates contained the LMP transaction screens that allowed users to record the receipt of goods or services function (MIGO or ZIGO). Of the 13 FSR templates, 7 contained inherent segregation of duties conflicts. For example, the FSR template "R/3 IMWM Goods Movement" inappropriately allowed the Receiving Specialist, MRP Planner/Buyer, or Warehouse Specialist to change a purchase order (ME22N), record the receipt of goods or services (MIGO or ZIGO), transfer goods (MB1B), and adjust the inventory within the warehouse (MB1A). The combination of these transaction screens created a vulnerability to unauthorized and fraudulent transactions because LMP users with this access could change purchase orders, enter the goods receipts, and change inventory records. The two AWCF activities we visited had assigned 624 users one or more of these seven FSR templates, which contained the ZIGO or MIGO transaction screens and another transaction screen that created an inherent segregation of duties conflict. Appendix F explains the potential segregation of duties conflicts that could exist within the P2P business process, and Table F-1 identifies the LMP transaction screens that could pose conflicts. Because Army managers did not define the FSR requirements and identify potential conflicts, the UAM managers did not have the ability to train their administrators and supervisors on how to assign system access correctly.

> *The two AWCF activities we visited had assigned 624 users one or more of these seven FSR templates, which contained the ZIGO or MIGO transaction screens and another transaction screen that created an inherent segregation of duties conflict.*

In addition, some FSR templates did not comply with specific laws and regulations to ensure the system maintained data integrity. For example, commanders at both the LCMC and Depot did not ensure that the process to assign 13 FSRs that performed receipt of goods or services function (MIGO and ZIGO) was assigned to only those individuals appointed in writing as a Designated Accountable Official by the LMP activity's commander. This written appointment was necessary to comply with DoD FMR, volume 5, chapter 33, "Certifying Officers, Departmental Accountable Officials and Review Officials," August 2010. UAM administrators or supervisors were then able to validate that the users were appointed to fulfill this requirement before granting them access to perform these functions. As a result, the LMP activities had not implemented the requirements of the Certifying Officers' Legislation and could not hold the LMP users performing receipt and acceptance functions accountable for improper payments resulting from the data they provided to entitlement systems. Without identifying the conflicts and other regulatory requirements needed to perform business events within LMP, activities unknowingly subjected LMP to data integrity problems and potential compromise. Army

managers should determine the impact of regulatory requirements, such as the Departmental Accountable Official Legislation, on the development and issuance of FSR templates. Supervisors and system administrators should ensure the proper appointment of all users before granting access to the templates.

Developing a Risk Matrix of Potential Conflicts

Army managers did not develop a risk matrix that assessed the assignment of LMP transaction screens within templates used during the P2P business process for potential segregation of duties conflicts. The BEA business rules provided specific guidance on how functions related to the P2P business process needed to be assigned and highlighted potential segregation of duties conflicts that could exist. Army managers did not assess the risk of assigning each of the LMP transaction screens used in the P2P business process to ensure that the LMP Project Office developed FSR templates that segregated duties correctly. Army managers should have developed a risk matrix, which identified each transaction screen within the P2P business process and highlighted transaction screens, when assigned together, would create a segregation of duties conflict. Table 2 is a sample of risk matrix related to the LMP P2P business process in which a dot denotes pairs of transaction screens that would create a conflict if assigned to the same user.

Table 2. P2P Transaction Screen Risk Matrix

LMP Screen	ME51N	ME52N	MIGO	ZIGO	XK01
ME51N			•	•	•
ME52N			•	•	•
MIGO	•	•			•
ZIGO	•	•			•
XK01	•	•	•	•	

Army managers should have worked with LMP personnel to map the templates to the P2P business process and identify which FSR templates, when assigned together, would create conflicts. For example, as shown in Table 2, LMP users who could record the receipt goods and services (MIGO and ZIGO) should not also have access to create or modify purchase requests (ME51N or ME52N) or update the Vendor Master (XK01) to prevent unauthorized transactions that could go undetected. Army managers should then have determined whether they needed to separate the functional authorities in the templates to prevent segregation of duties conflicts or develop compensating controls to monitor the potential conflict created within the template. Army managers should perform a risk assessment of the LMP transaction screens assigned within the FSR templates to minimize the potential for segregation of duties conflicts.

Assigning Users Multiple Functional Security Role Templates Resulted in Conflicts

UAM administrators and supervisors created additional segregation of duties and least privilege conflicts when assigning the FSR templates to employees. At the two activities visited, UAM administrators and supervisors stated that they were unaware of a requirement to administer FSR templates based upon segregation of duties and least privilege concepts, and they did not know which FSR templates could create a conflict. As of November 2010, UAM administrators at the two activities visited had assigned 10 or more FSRs to 1,998 of the 3,513 LMP users, while more than 850 of the 3,513 LMP users had 25 or more FSRs assigned to them. Although users required a certain number of FSRs to accomplish day-to-day tasks, the assignment of 25 or more FSRs appeared to indicate that Army managers did not design the FSR templates properly for conducting the LMP business process and did not achieve the role-based system access control needed to maintain data integrity.

The assignment of multiple FSRs to a user could create a least privilege conflict if they were not necessary for the individual to perform job responsibilities. For example, the Depot assigned one user the FSR "R/3 IMWM [Restricted] CCI Movement." This FSR allowed for the transfer of cryptographic items. Of the transactions available within this FSR template, the user informed us that they only required transaction screen ZMMBE (Stock Overview). However, the template also contained access to transaction screens to create and modify purchase orders (ME21N and ME22N), create equipment (IE01) as used within plant maintenance, and change outbound delivery documents (VLO2N). The user did not require any of these transaction screens to perform her job. The assignment of excess access caused a least privilege conflict. The need for most users to have the functional authorities in multiple FSR templates demonstrated that Army managers had not effectively mapped the FSR templates to the P2P business process. They also did not provide the UAM administrators and user supervisors with sufficient guidance on how to assign multiple FSR templates to an individual user without causing least privilege and segregation of duties conflicts.

AMC personnel should map each FSR template created to the BEA P2P process to determine the existence of potential segregation of duty and least privilege conflicts. If conflicts exist, they should reassign the transaction screens to other FSR templates as necessary to prevent conflicts. Once this assessment is completed, managers should redesign the templates to cover the specific job functions performed at each LMP activity and limit user access to only those transaction screens needed to perform specific functions.

Implementing Other System Controls to Prevent Conflict

AMC managers stated that they had not developed or implemented other types of LMP system controls that would prevent UAM administrators and supervisors from assigning FSRs, that when combined, created conflicts. The commercial software package contains a Governance, Risk, and Compliance module, which helps prevent unauthorized access and achieve real time visibility into access risk. Army managers stated that they have identified the need for the module but have not yet funded its purchase. AMC should either purchase the system software or identify and develop other system controls needed to assist in identifying excessive or unauthorized access.

Developing Consistent Account Management Policy and Procedures

Although AMC developed an LMP User Access Policy, it did not provide LMP activities with the detailed procedures to implement the policy. The LMP User Access Policy did not identify a preferred method for controlling system access, assigning FSRs to users based on specific job descriptions, or defining FSR templates that when assigned together created potential segregation of duties or least privilege conflicts. In addition, the policy did not contain adequate procedures to ensure that the UAM administrators implemented the NIST account management requirements. NIST requires that an information system have the ability to identify authorized system users and specify user access privileges. NIST also requires appropriate officials to establish accounts and for organizations to activate, modify, disable, and remove accounts and notify account managers when users are terminated or transferred and deactivate accounts of terminated or transferred users. The two LMP activities visited developed unique procedures for administering user access. The Depot and LCMC did not consistently or appropriately:

> *The LMP User Access Policy did not identify a preferred method for controlling system access, assigning FSRs to users based on specific job descriptions, or defining FSR templates that when assigned together created potential segregation of duties or least privilege conflicts.*

- administer the management of user FSRs,
- adjust access based on changing job assignments,
- remove access when an individual left the organization or lost their security clearance, or
- review assigned user access on a regular basis.

There was also a lack of consistency on how the two activities performed UAM account management. The Depot employed a single part-time UAM administrator who used a mostly manual process to manage LMP user access. The six full-time UAM administrators at the LCMC used an offline database to track supervisor approval and manage LMP user access. Both activities had control weaknesses in how the UAM administrators controlled system access.

Letterkenny Army Depot System Access

The Depot UAM administrators and managers did not effectively establish and maintain user access. As of November 1, 2010, the Depot UAM administrator had assigned 943 users between

2 and 95 of the 179 FSR templates that Depot managers determined applicable for use. Of those 943 users, 254 users had 25 or more FSRs assigned to them. The Depot used a mostly manual process for granting system access that started with the supervisor submitting a request form to the UAM administrator. The UAM administrator reviewed the FSRs in the request and routinely granted the system access unless the supervisor requested "Restricted" FSRs. The UAM administrator forwarded any requests for "Restricted" FSRs to the Depot's LMP Transformation Chief for additional approval. However, the UAM administrator did not maintain an automated database that supervisors could use to identify the FSRs already assigned to an employee. In addition, there was no automated method to notify the UAM administrator when users left the Depot or changed assignments that affected the FSR assignments.

To assist us in determining whether adequate LMP system access controls existed at the Depot, we surveyed a sample of the 943 user accounts. See Appendix G for details on how we conducted the survey. Although most users thought they had the access needed to perform their jobs, we estimated that:

- 391 users were unaware of all the FSRs and transaction screens assigned to them (a potential least privilege conflict),
- 885 users had at least one FSR assigned that they did not use (a potential least privilege conflict), and
- 140 users had potential segregation of duties conflicts. For example, some users had the ability to create and update purchase requests and purchase orders and receive goods. Other respondents could perform purchasing functions as well as receive, accept, transfer, and write-off goods.[14]

The UAM administrator was also able to assign FSRs to herself. She had this access to perform the other tasks assigned to her, such as working with the material master, clearing transactions, and making mass updates of information within the system (system cleansing). LMP Project Office and AMC G-3 personnel stated that there was no policy prohibiting UAM administrators from assigning access to themselves. These personnel also stated that other LMP activities allowed UAM administrators to assign FSRs to themselves to perform activity workload. AMC managers could not identify any compensating controls they implemented to monitor the FSRs assigned to the Depot's UAM administrator. The ability of the UAM administrators to assign FSRs to themselves without higher level monitoring makes LMP data vulnerable to fraud and abuse that could go undetected by Army managers. AMC G-3 should work with LMP activities to control UAM administrator roles and prevent administrators from assigning FSRs to themselves, or develop appropriate compensatory controls.

Aviation and Missile Life Cycle Management Command System Access

The LCMC did not implement effective LMP account management for establishing and maintaining user access. As of October 18, 2010, the LCMC UAM administrators had assigned 2,570 users between 1 and 95 of the 162 FSR templates determined applicable for use by LCMC

[14] See Appendix G for sample methodology and projections.

personnel. The LCMC had an offline database that tracked user access requests and supervisor approvals. However, the UAM administrators did not keep the information in the database up-to-date, making the offline database an ineffective tool for managing accounts. Interviews with a limited number of users, supervisors, and UAM administrators, and reviews of documentation identified the following control weaknesses.

- By assigning users more FSRs than they needed to perform their assigned functions, UAM administrators and supervisors caused least privilege conflicts.

- UAM administrators did not reconcile the FSR information between the offline database and LMP. As a result, the access contained in the offline approval database did not always match what the administrator had actually granted in LMP. For example, an individual to whom the administrator had assigned 95 FSRs in LMP, had only 61 FSRs assigned by the supervisor in the offline database. The discrepancy occurred when the UAM administrator removed a user's access from the offline database upon reassignment of the individual to a new supervisor. However, the UAM administrator did not remove the access to the FSRs from LMP. Consequently, the user had more system access than intended.

Adjusting System Access for Reassigned User

The LMP User Access Policy did not provide UAM administrators and user supervisors with the detailed procedures they needed to ensure that activities controlled the reassignment of LMP users. The LMP User Access Policy directed supervisors to review assigned FSRs periodically and, based on that review, request necessary changes to user access. However, supervisors were not routinely informing the UAM administrators that a user's access to FSRs was no longer needed and required removal. At both activities visited, problems existed with how supervisors implemented the policy. For example:

- Supervisors allowed users to accumulate a large number of FSRs as they transferred between job assignments within the activity. Former supervisors generally did not request the removal of the FSRs assigned to a user before the user departed an activity, and the acquiring supervisor did not review the FSR templates previously assigned to a user before approving access to additional FSRs for that user. For example, we identified a user reassigned from an inventory management function to accounts receivable and project management function. The user's supervisor did not notify the UAM administrator of the job change so that the UAM administrator could adjust the FSRs assigned to the user. The combination assigned to this user provided the user with excessive access. The user, who had access to the cash receipt and allocation transactions, had the ability to create customer orders, purchase orders, receipt of goods, and inventory adjustments. The user could also generate letters requesting customer payment. The UAM administrator removed the extra access when notified of this situation. However, the user could have performed system actions that might have resulted in a loss of funds or misappropriation of assets.

- UAM administrators did not routinely review the accuracy of the information in the offline database or use other tracking mechanisms to ensure that users did not have extra

access. A review conducted by the LCMC UAM administrators identified 79 users who had been assigned to more than one office by the LCMC. The UAM administrators took immediate actions to adjust the access provided to the 79 users.

- User access was not consistent with the tasks assigned. For example, a user at the LCMC, whose main responsibility was to enter high priority requests for repair parts from stock on hand within the LMP sales order module, also had FSRs to create and change certain types of purchase requisitions and purchase orders, receive goods, return goods to vendors, and dispose of goods. This user had no need to perform any of these additional functions. This happened because supervisors granted users more access than required for their assigned functions. In addition, UAM administrators did not review user access recorded in the offline database closely enough to identify access no longer required.

Army Materiel Command Activities Were Not Performing Periodic Access Reviews of Logistics Modernization Program System Access

Managers at all levels did not conduct periodic reviews of LMP system access placing the system at risk for potential misuse. The NIST standard requires that organizations define the frequency of conducting user access reviews. The LMP User Access Policy states that LMP activities should conduct system access reviews on an annual basis. However, neither the two LMP activities visited nor Army managers were able to provide documentation showing that they had conducted reviews of system access. UAM administrators confirmed that it was the supervisor's responsibility to review system access. However, the supervisors we spoke with at the two activities visited stated that they were unaware of the requirement for periodic reviews.

User Access Removal Was Not Properly Performed

LMP User Access Policy directed supervisors to request removal of access for all employees leaving their work unit through transfer or termination or because of the loss of their security clearance. Supervisors at the two activities were not routinely removing LMP system access as required, including those users that were inactive. At the Depot, 4 of 78 sampled users had left the Depot or had their security clearance removed between February 1, 2010, and September 30, 2010, but still had an LMP access account as of November 1, 2010. The UAM administrator removed the four user accounts when we informed her of the situation. This lack of control places the system at risk for potential misuse. Depot records showed that 265 of the 943 total user accounts were in an inactive status. There was no documentation showing which accounts required permanent deactivation or were simply inactive due to non-use. LMP automatically placed a user in inactive status after 90 days of inactivity. System access procedures require a review at regular intervals of all user accounts suspended due to inactivity. The UAM administrator should have conducted a review of inactive users to determine whether the users still required system access or if they had left the Depot and their user account required permanent deactivation. Not performing this function demonstrated ineffective account management. The Depot UAM administrator stated that she did not conduct

> *Depot records showed that 265 of the 943 total user accounts were in an inactive status.*

reviews and that inactive users remained within LMP until Human Resources Office personnel or a supervisor notified the administrator that the Depot had reassigned the user or the user had departed the Depot.

The LCMC UAM administrators also did not have a procedure in place to monitor users in an inactive status. As of April 6, 2011, the LCMC had 1,448 inactive system access accounts. As of June 30, 2011, 21,620 users had LMP system access. However, LMP had suspended 7,787 system access accounts due to inactivity. In response to our audit concerns, the two activities updated some of their user access and removed inactive users. As of August 4, 2011, the Depot had reduced the number of total users from 943 to 725 and reduced inactive users from 265 to 48. As of August 8, 2011, the LCMC had 1,361 inactive users.

> *As of June 30, 2011, 21,620 users had LMP system access. However, LMP had suspended 7,787 system access accounts due to inactivity.*

While the LMP User Access Policy does not specifically address the need for the UAM administrators to review inactive accounts, Army Regulation 25-2, "Information Assurance," October 24, 2007, requires information assurance support personnel to terminate inactive accounts verified as no longer required after 45 days. The LMP User Access Policy should require the UAM administrator to perform regular reviews of system access accounts suspended due to inactivity. UAM administrators should work with supervisors to ensure that users have the access they require and to remove unneeded user access accounts from the system.

User Access Oversight Was Not Effective

Army managers did not provide sufficient oversight of LMP user access. Army managers had not developed the guidance and internal control checklists or other control documentation required to assess compliance with LMP access policies. Additionally, no one at any level could provide documentation for any review performed of system access controls since LMP implementation in July 2003. Headquarters, AMC Internal Review Office personnel stated that they had not yet developed a program for assessing LMP system access controls. Without a robust internal control review process to monitor LMP user access, LMP managers had limited assurance that they developed adequate system controls that were operational effective to monitor system access requirements. ASA(FM&C) should work with AMC to develop the standards and guidance for implementing and monitoring the internal control requirements for account management, segregation of duties, and least privilege.

Army Materiel Command Taking Actions to Update Account Management

In March 2011, AMC personnel stated that they were revising the LMP User Access Policy. The new policy was to contain updated procedures to assist UAM managers in effectively managing LMP system access controls. Once updated, AMC personnel stated that they would be providing additional training on the new policy to UAM managers, UAM administrators, and activity personnel. They also stated that AMC had assembled a team to create internal control checklists

for activities to use in assessing system access controls. These actions are necessary to strengthen the process and more consistently administer the LMP system access policy. AMC plans to issue a new access policy in FY 2012.

To help ensure the consistent administration of system access, AMC should supplement the updated policy with detailed procedures on how UAM administrators and supervisors should assign FSRs to users. The procedures should provide for the use of an automated database, such as the one used at the LCMC, to track system access approvals and reconcile to FSRs granted to users in LMP. AMC should develop procedures to ensure notification of the UAM administrators of any personnel action that could result in adjusting an LMP user's access. The procedures should require the appointment of at least one full-time UAM administrator at each activity who is responsible for monitoring system access daily, resolving problems such as system inactivity, and validating that approved roles do not create conflicts. Once AMC updates the LMP User Access Policy with detailed procedures, UAM managers should train UAM administrators and supervisors on how to properly assign user FSRs and assess the templates to determine if specific functional roles must be modified or new templates created to perform the activities mission. In addition, AMC should periodically provide centralized training on FSR administration for all UAM managers, UAM administrators, and user supervisors—specifically, training on account management, segregation of duty, and least privilege controls.

Conclusion

LMP FSRs and other system controls did not properly safeguard P2P data processing. Army managers did not develop a risk matrix that assessed the assignment of LMP transaction screens within FSR templates, and the processes used to develop and implement the FSRs did not establish controls over segregation of duties and least privilege conflicts. AMC had issued an LMP User Access Policy. However, the policy did not have sufficient detail to ensure that UAM administrators and user supervisors could effectively administer user access. The policy did not identify a preferred method for assigning FSRs to users or define FSR combinations that could create segregation of duties or least privilege conflicts. UAM administrators and supervisors at the two activities visited, assigned multiple FSRs to individuals that could result in conflicts.

The two activities did not perform consistent or effective account management, to include assigning at least one full-time UAM administrator to administer user access, developing common procedures and databases for administering the approval process, conducting regular access reviews, and assessing inactive accounts for removal. Managers at all levels did not perform periodic reviews of LMP system access. As a result, Army managers have subjected LMP data to an increased vulnerability to unauthorized and fraudulent transactions. AMC has recognized the need to strengthen system access controls. AMC plans to update procedures for account management, segregating duties, and limiting access to the extent necessary to perform duties. However, Army managers still need to reassess the development of their FSR templates and map them to each of the BEA business processes to determine the controls needed to prevent conflicts that could result in potential fraud, waste, and abuse. They also need to improve system access controls by reviewing and assessing the impact that regulatory requirements and risk assessment associated with assigning transaction screens have on the FSR templates developed. They should ensure that the procedures developed are maintained and provide the UAM managers and administrators the information they require to administer system access correctly.

Once they redesign the FSRs templates, the ASA(FM&C) and AMC G-3 should perform a one-time review of LMP access to identify and resolve segregation of duties and least privilege conflicts.

Recommendations, Management Comments, and Our Response

B.1. We recommend that the Assistant Secretary of the Army (Financial Management and Comptroller) develop a plan for the Army Materiel Command to improve system access controls within the Logistics Modernization Program system. Specifically:

a. Determine the impact of regulatory requirements, such as the Certifying Officer's Legislation, on the development and issuance of the functional security role templates. Within 60 days of the report, identify and correct missing and deficient official appointment documentation before allowing access to the templates. Once identified, supervisors and system administrators should ensure the proper appointment of users before granting access to the templates containing those functions.

Department of the Army Comments

The ASA(FM&C) agreed and stated that she will direct Headquarters AMC and DFAS to perform a comprehensive review in March 2012 of LMP system controls. The review will cover access controls, interface controls, process controls, configuration controls, and data integrity. The purpose of the review will be to identify system access deficiencies and risk and provide an approach for addressing deficiencies. The ASA(FM&C) also stated that Army managers are in the process of reviewing appointment documentation and additional requirements will be identified in the plan of action and milestones.

Our Response

The Army comments were partially responsive. The Army did not specifically address that the review would identify regulatory requirements, such as the Certifying Officer's Legislation, on the development and issuance of FSR templates. We request that the ASA(FM&C) reconsider her response to this recommendation and provide additional comments on the final report, explaining how she will restrict system access until proper appointment documents are completed to ensure proper accountability over payment certification functions. The additional comments should also identify a date for completing the review of appointment documentation and correcting missing and deficient documentation.

b. Perform a risk assessment of the Logistics Modernization Program system transaction screens assigned within each of the functional security role templates and minimize the potential for segregation of duties conflicts. Once this assessment is completed, managers should redesign the templates to cover the specific job functions performed at each activity and limit user access to only those transaction screens needed to perform those job functions.

Department of the Army Comments

The ASA(FM&C) agreed and stated that she will direct Headquarters AMC and DFAS to perform a comprehensive review of LMP system controls. The review will cover a wide-range of controls and will include necessary risk assessments and other tools and techniques to assess and appropriately limit user access.

Our Response

The Army comments were responsive.

c. Require the mapping of each functional security role template to the Procure-to-Pay business process to determine the existence of potential segregation of duty and least privilege conflicts. If conflicts exist, realign the transaction screens as necessary to prevent these conflicts.

Department of the Army Comments

The ASA(FM&C) agreed and stated that the Army and Headquarters AMC will provide business rules for handling segregation of duty conflicts when updating the FSRs. The ASA(FM&C) stated that until Governance, Risk, and Compliance functionality is implemented, the Army will continue to use existing meetings and policy to minimize conflicts. In response to Recommendation B.2, the ASA(FM&C) stated that the Army plans to begin configuration of that functionality in February 2012, with a release date of December 2012. To minimize the risk of conflicts, FSRs will be reviewed and, if necessary, redesigned after Governance, Risk, and Compliance implementation.

Our Response

The Army comments were responsive.

d. Update the Logistics Modernization Program User Access Policy and include detailed procedures that prescribe:

(1) How administrators and supervisors should assign functional security roles to users.

(2) How to manage user access to include the use of approval databases or another tracking mechanism.

(3) How administrators should perform regular review of system access accounts suspended due to inactivity and work with supervisors to suspend or remove all roles when a user departs a work unit, leaves an activity installation, or loses a security clearance and obtain approval by the new supervisor of all access granted after reassignment.

Department of the Army Comments

The ASA(FM&C) agreed and stated that the Headquarters AMC Chief Information Officer signed an updated User Account Manager Policy on January 24, 2012. The ASA(FM&C) stated that the new policy requires the review of all suspended and inactive accounts on an annual basis. The ASA(FM&C) also stated that managers and supervisors receive training on the use of the UAM system on a regular and ad hoc basis as system and personnel changes occur. Additionally, she stated that policy updates will be made as a result of system access reviews. In response to Recommendation B.2, the ASA(FM&C) stated that the new policy addresses how managers and supervisors assigned FSRs.

Our Response

The Army comments were generally responsive. Headquarters AMC provided us a copy of the updated User Account Manager Policy. Although the ASA(FM&C) did not address how the Army would manage user access, the updated policy identified how AMC would use a system access tool to manage user access. No further comments are required.

e. Conduct an initial review of system access, at all levels, to identify users who have been granted unneeded access and, thereafter, conduct periodic reviews of system access.

Department of the Army Comments

The ASA(FM&C) agreed and stated that the Army and Headquarters AMC will provide business rules for handling segregation of duty conflicts when updating FSRs. In response to Recommendation B.2, the ASA(FM&C) also stated that the Headquarters AMC Chief Information Officer will instruct activities on how to conduct an annual UAM review during the third quarter of FY 2012. She also stated that Headquarters AMC Chief Information Officer personnel will conduct periodic reviews to ensure UAMs are not assigning themselves privileges and will take action for users violating their privileges.

Our Response

The Army comments were responsive.

f. Develop a method to monitor the assignment of functional security roles at the highest level and ensure that activities conduct the required periodic reviews.

Department of the Army Comments

The ASA(FM&C) agreed and stated that she will direct Headquarters AMC and DFAS to perform a comprehensive review of LMP system controls. In response to Recommendation B.2, the ASA(FM&C) stated that the updated User Account Manager Policy now addresses FSR assignments and the mitigation of segregation of duties conflicts.

Our Response

The Army comments were responsive.

B.2. We recommend that the Assistant Secretary of the Army (Financial Management and Comptroller) work with the Army Materiel Command to:

a. Provide centralized training for administrators and supervisors on how to use functional security role templates to administer access and prevent conflicts.

b. Purchase the system software needed to assist in developing the system controls needed to prevent or identify excessive or unauthorized access, or identify and develop compatible system controls using other means.

c. Control administrator roles and prevent administrators from assigning functional security roles to themselves or develop appropriate compensating controls.

Department of the Army Comments

The ASA(FM&C) agreed and stated that upon completing the system access review in Recommendation B.1, the Army will be in better position to identify training requirements, target audiences, and the right automated tool to handle provisioning of users and controlling system roles and permissions. Within 60 days of the review, Army and Headquarters AMC will review current training requirements and adjust them accordingly. The ASA(FM&C) stated that the updated AMC User Account Manager Policy addresses FSR assignments and the mitigation of segregation of duties conflicts, and additional corrective requirements will be addressed as part of the development of a plan of action and milestones. She also stated that the Army has plans to begin configuration of the Governance, Risk, and Compliance functionality in February 2012, with an implementation date of December 2012. The functionality will proactively mitigate risk and provide the system controls needed to prevent or identify excessive or unauthorized access and segregation of duties conflicts. FSRs will be reviewed and, if necessary, redesigned after Governance, Risk, and Compliance implementation to minimize risk. Finally, the ASA(FM&C) stated that the Headquarters AMC Chief Information Officer will conduct periodic reviews to ensure UAM administrators are not assigning themselves privileges and will take action for any users violating their privileges.

Our Response

The Army comments were responsive.

Finding C. Vendor Master Data Did Not Support the Procure-to-Pay Process

Army Enterprise Systems Integration Program (AESIP) personnel did not determine the Standard Financial Information Structure (SFIS) attributes needed to establish records in a vendor master database and populate the correct domain values for Army ERP and other systems to process P2P transactions correctly. This occurred because the Army OBT and ASA(FM&C):

- did not direct the AESIP Program Management Office to function as the single source of Army vendor master information or require AESIP personnel to develop, manage, and maintain the Army's vendor master for use throughout the Army's ERP environment; and
- allowed Army ERP program managers to develop their own methodologies for deriving vendor data. [15]

As a result, Army ERP program managers have spent or intend to spend about $1.3 million to develop unique functionality to derive vendor information in their own systems, but did not resolve long standing material weaknesses related to accounts payable and intragovernmental eliminations.

Vendor Master Information Requirements

SFIS is the comprehensive "common business language" that supports DoD information and data requirements for budgeting, financial accounting, cost and performance management, and external reporting across the enterprise. SFIS enables decision-makers to compare the cost of programs and their associated activities and provides a basis for common valuation of DoD programs, assets, and liabilities. The SFIS Transaction Library and accompanying SFIS matrix provided DoD activities with the specific attributes, domain values, and business rules needed to populate DoD accounting transactions correctly. The Glossary defines attributes, business rules, and domain values. The SFIS matrix, version 8.0, March 2011, contained the business rules and attributes required for implementing standard transactional domain values within DoD systems, including three attributes that identified business partner information.[16] The SFIS business rules required ERP systems to store and maintain the attributes and the domain values. A vendor master database uses internal unique identification codes to aggregate and build table data on which to base all functionality for ERP systems' master data management. Table 3 identifies the three SFIS Trading Partner Information attributes and their valid domain values.

---

[15] Although this report addresses issues with the implementation of LMP, the solutions developed within AESIP also affect GFEBS use of the vendor master database. We identified similar issues with how GFEBS personnel requested and used vendor master data. Reference to Army ERP program managers includes both the LMP project manager and GFEBS program manager.

[16] DoD issued SFIS matrix version 7.0 in March 2010. It contained 72 attributes. SFIS matrix version 8.0 reduced the number of attributes to 66. During this audit, we reviewed business rules for the business partner information in both versions of the SFIS matrices and found no differences. Business partner information relates to commercial vendors and other trading partners.

Table 3. SFIS Trading Partner Information Attributes and Domain Values

Attribute		Domain Values Information	
Key	**Name**	**Values**	**Description**
TP1	Federal/Non-Federal Indicator	F	Other Federal entities
		N	Non-Federal entities, such as private business or local, state, tribal, and foreign governments
TP2	Trading Partner Indicator Code	3-digit code	Other Federal entity Department Regular Code as determined by the Department of the Treasury
TP3	Business Partner Number	9-digit Data Universal Numbering System number	All business partners except DoD entities
		"DOD" followed by a 6-digit DoD Activity Address Code	DoD entities

Determining Standard Financial Information Structure Domain Values and Business Partner Registration Status

The General Services Administration established the Business Partner Network (BPN) as the single source for obtaining business partner information. The network provided direct access to the two databases the Government used to register its business partners: the Federal Agency Registration (FedReg) and Central Contractor Registration (CCR).

Federal Agency Registration Requirements

Treasury Financial Manual Bulletin No. 2011-04, "Intragovernmental Business Rules," November 8, 2010, requires Federal agencies that conduct business transactions with other Federal agencies to obtain and use a unique BPN number and register it in the FedReg.[17] Federal business partners must access the FedReg at least annually to validate and update their BPN information.

Central Contractor Registration Requirements

The CCR is the primary registry for non-Federal business partners. The Federal Acquisition Regulation requires both current and potential business partners to register in CCR to do business with DoD financial and acquisition activities. It requires registrants to enter all mandatory CCR information, including their Data Universal Numbering System number. It also required Government personnel to validate all mandatory fields, including a validation of the taxpayer identification number, with the Internal Revenue Service, before activating the CCR record. To keep their registrations active, registrants must renew and revalidate their registration annually

[17] Treasury Financial Manual Bulletin No. 2007-03, October 2006, established the BPN requirement. Treasury Financial Manual Bulletin No. 2011-04 superseded the previous version.

and maintain an active status until the government makes all payments to them on outstanding contracts. The CCR User Guide requires registrants to categorize their organization as Federal, state, local, tribal, or foreign governmental entity, or a private business.

Developing a Single Army Vendor Master

In November 2007, after the Army began ERP deployment, the Army identified the need to develop AESIP as the integration program and authoritative source for its master data.[18] The Army spent or planned to spend $242.8 million to develop AESIP as its vendor master data manager. However, AESIP personnel did not determine the SFIS attributes needed in a vendor master database to populate the correct domain values for Army ERP and other systems performing P2P functions to process transactions correctly. This occurred because the Army OBT and ASA(FM&C) did not direct the AESIP Program Management Office to function as the single source of Army vendor master data information or require AESIP personnel to develop, manage, and maintain the Army's vendor master for use throughout the Army's ERP environment.

> *. . . AESIP personnel did not determine the SFIS attributes needed in a vendor master database to populate the correct domain values for Army ERP and other systems performing P2P functions to process transactions correctly.*

The Army ERP Strategy reaffirmed the need for a vendor master database to maintain a single source of Army business partner information.[19] Previously, Army ERP program managers developed their own methodologies for establishing vendor tables for use within their respective system. These methodologies incorrectly established the three required SFIS attributes related to business partner information, which prevented them from accurately identifying business partners and properly recording Federal and non-Federal business transactions.

Establishing Business Partner Records Using the Business Partner Network Number

Although the Army designed AESIP to provide and sustain the hub services capability needed to facilitate ERP integration, AESIP personnel had not assumed the responsibility needed to become the single authoritative source of trading partner information as contained in its mission statement. In addition, they did not develop the vendor master using the SFIS Trading Partner Information attributes and domain values for establishing business partner records. Therefore, AESIP personnel did not establish the business partner number (TP3) domain values as the primary data field for establishing business partner records in the vendor master data. Instead,

---

[18] Army managers originally established AESIP as Product Lifecycle Management Plus in FY 2004, and renamed it to AESIP in FY 2008. In November 2007, the Product Lifecycle Management Plus implemented a Customer and Vendor Master data capability. In 2007 and 2008, the Army logistics community accomplished a three-phased ERP Integration Analysis Study, which evaluated the best way to execute and integrate GFEBS, LMP, and Product Lifecycle Management Plus. The study recommended a Federated ERP integration approach to leverage Product Lifecycle Management Plus for Business Intelligence, Business Warehousing, and Master Data Management.

[19] The Army ERP Strategy defined the Army ERP environment as containing four ERP systems: LMP, GFEBS, Global Combat Support System-Army, and Integrated Personnel and Pay System-Army. The Army ERP Strategy used AESIP to integrate the business processes and data needed to accomplish business events within the Army ERP systems.

AESIP personnel used a legacy process that established the records using a business partner's Commercial and Government Entity (CAGE) code or Routing Identifier Code. AESIP needed to use the BPN to obtain its business partner information and cease obtaining vendor registration information from other sources.

The Government developed the BPN databases (FedReg and CCR) to serve as the single source for Government business partner information. The SFIS TP3 attribute was to provide a unique identification for each business partner. DoD originally used databases for CAGE codes or Routing Identifier Codes to uniquely identify business partners and provide similar information. In November 2007, AESIP personnel began receiving domain values from the BPN databases. However, AESIP personnel continued to use the CAGE code or Routing Identifier Code to establish the individual business partner record in the vendor master instead of establishing vendor master records using the BPN number provided by the databases as required by SFIS. If they had established the vendor master using the BPN number, they could have then obtained any additional information needed from such sources as the CAGE code or Routing Identifier Code databases using the TP3 domain value.[20] If not registered in FedReg, AESIP personnel should have required the business partner to register before establishing a vendor master record for that business partner.

Despite having received the required TP3 domain values from the FedReg and CCR databases, the AESIP program manager did not establish a BPN number field in the vendor master structure to use as the primary field needed to establish each vendor master record. Based on the information received by BPN number from the BPN databases, the AESIP program managers should also have been able to record an appropriate Federal and Non-Federal Indicator (TP1) and Trading Partner Indicator Code (TP2) domain value for each business partner established in the Army's vendor master database. Appendix H describes how the Army should develop a vendor master database using the three SFIS business partner attributes. Table H-1 provides the SFIS attribute data, required source data, and AESIP data field requirements. To ensure that Army ERP systems, and other systems performing P2P functions, provide the required SFIS business partner attributes information, the AESIP program manager should develop the AESIP data fields identified in Table H-1 within the Army vendor master database to record the three required SFIS attributes. AESIP personnel should create all business partner records from information contained in the Federal Agency Registration and Central Contractor Registration. AESIP should establish individual business partner records using the BPN number and create data files to populate the applicable SFIS attributes. Since the BPN has become the single source of business partner information, DCMO should work with the Under Secretary of Defense (Comptroller) to reevaluate the use of legacy registration processes such as the CAGE code and

Based on the information received by BPN number from the BPN databases, the AESIP program managers should also have been able to record an appropriate Federal and Non-Federal Indicator (TP1) and Trading Partner Indicator Code (TP2) domain value for each business partner established in the Army's vendor master database.

[20] AESIP needs to be able to create records for business partners not required to register in one of the BPN databases using a unique 9-digit Data Universal Numbering System number.

Routing Identifier Code databases for tracking business partner information and determine whether DoD can eliminate these databases by merging them with the BPN databases. Army OBT and ASA(FM&C) should require each Routing Identifier Code location to register in FedReg before allowing AESIP to create a business partner record in the Army vendor master or accepting any supplemental business partner information from that location.

Army Enterprise Systems Integration Program Needed to Provide More Effective Data Management

The Army ERP Strategy reaffirmed AESIP as the single source of authoritative data for developing a common vendor master database for use by all Army systems. However, in the Army ERP Strategy, Army OBT did not require the AESIP program manager to assume the authority for master data and direct the use of the data by all Army systems. The AESIP program manager did not develop the vendor master data using the BPN number that would allow for the capture of SFIS attributes for vendors and pass information to systems such as LMP. AESIP personnel simply passed vendor information from CCR to LMP and did not assume the authoritative control over that information. AESIP personnel stated that the LMP Project Office was responsible for requesting the appropriate AESIP business partner information.

> *The AESIP program manager did not develop the vendor master data using the BPN number that would allow for the capture of SFIS attributes for vendors and pass the information to systems such as LMP.*

AESIP personnel provided the LMP Project Office with a listing of the AESIP vendor master data fields. LMP personnel determined the fields needed and provided the system mapping requirements and commercial software layout structure of the targeted fields to AESIP personnel. The AESIP personnel mapped the data fields as the LMP personnel requested and provided the vendor information to the system. However, the methodology designed by LMP personnel was flawed. Specifically, the LMP personnel did not request the proper data from AESIP to record the SFIS Federal/Non-Federal Indicator attribute (TP1).

Incorrect Derivation of Federal/Non-Federal Indicator

Our review of the 2.3 million LMP vendor records that existed as January 4, 2011, showed that LMP incorrectly classified Federal and non-Federal business partners. This occurred because the LMP personnel derived the TP1 domain values for business partners using an incorrect methodology. The methodology used derived the TP1 domain value based on whether the business partner information received by LMP contained a DoD Address Activity Code (DoDAAC) number. If the information contained a DoDAAC number, the methodology classified that business partner with a domain value of “F” and recorded the transaction in the subsidiary ledger supporting Federal Accounts Payable (GLAC 2110.9100). Otherwise, the methodology classified the business partner with a domain value of “N” and recorded the transaction in the subsidiary ledger supporting non-Federal accounts payable (GLAC 2110.9200). This methodology was incorrect because LMP personnel based the determination of TP1 domain values on whether an activity had a DoDAAC number, rather than on the information contained in the FedReg and CCR. The misclassified portion of the LMP Federal and non-Federal business partners caused LMP to record all P2P transactions conducted with

those business partners incorrectly. For example, LMP recorded a non-Federal contractor as Federal because DoD had issued that contractor a DoDAAC number. Therefore, AWCF managers could not rely on the LMP information related to Accounts Payable and other related general ledger accounts to manage their activities with business partners and make intragovernmental eliminations.

Incorrect Use of Defaulted Trading Partner Indicator Domain Values

LMP Project Office personnel did not request the proper data field from FedReg for the Trading Partner Indicator Code attribute (TP2). Army managers should have directed the Army ERP program managers to request the Department Code of each Federal entity from FedReg. Instead, LMP Project Office personnel created their own methodologies to derive the information and did not derive accurate TP2 domain values. The LMP methodology incorrectly recorded a TP2 domain value of "99" for all business partners recorded in the subsidiary ledger supporting Federal Accounts Payable. This methodology caused the misclassification of all LMP transactions with these business partners because "99" did not represent the actual TP2 domain values for the business partners.[21] Problems in obtaining accurate TP2 domain values have prevented the Army from resolving its material weakness related to intragovernmental eliminations.

> *Army managers should have directed the Army ERP program managers to request the Department Code of each Federal entity from FedReg.*

Logistics Modernization Program System Did Not Use Trading Partner 3 Attribute Correctly

Army managers did not require the LMP Project Office to use the TP3 attribute as the primary data field to establish, populate, and maintain the vendor master and the domain values as each business partner's unique identifier. This occurred because Army managers believed that systems, such as LMP, were exempted from this requirement. However, BTA verified that the Army must use the TP3 domain values for unique identification of its business partners. Because LMP did not maintain TP3 domain values, it could not identify its business partner information as required by SFIS.

Business Program Number Registration Status Controls Disabled

LMP did not identify inactive business partners. LMP Project Office personnel stated that LMP had the capability to track the status of the CCR active records; however, they had turned off the CCR registration status controls in LMP because inaccurate information prevented them from making payments to business partners. By not using the CCR registration status controls, the LMP Project Office circumvented the system's control to prevent inactive business partners from receiving new contracts or additional payments.

---

[21] Trading Partner Indicator Code "99" did not represent a valid Department Regular Code.

Developing Vendor Master Data with Standard Financial Information Structure Attributes

To provide effective data management over the vendor master data process, the AESIP Program Management Office needs to assert its authority and create the vendor master data fields to establish unique business partner records based on the three SFIS trading partner information attributes obtained or derived from the BPN. As a data manager, AESIP needs to become the single-source for creating, updating, and deleting Army business partner records. Having a single source of Army vendor master data would control the vendor master data outside of the individual ERPs and add the appropriate internal control environment over the vendor master information used throughout the Army. The Army OBT and ASA(FM&C) should issue a policy appointing the AESIP program manager as the Army's vendor master data manager and require all systems doing business with the Army to use AESIP vendor master data. They should direct the AESIP program manager to issue instructions on the administration and use of Army vendor master data and ensure AESIP personnel validate the integrity of the business partner information. The ASA(FM&C) should also validate that LMP has controls in place to reject new contracts or payment requests from business partners with inactive registration flags.

Army Expended Funds to Develop Multiple Vendor Tables

The Army allowed Army ERP program managers to develop separate methodologies to derive their own vendor information. As of April 30, 2011, Army ERP program managers spent or planned to spend about $1.3 million to derive unique vendor master tables.[22] They used a portion of those funds to correct vendor information in the system. However, these efforts did not provide the SFIS trading partner information necessary to help resolve the Army's material weaknesses related to its accounts payable and intragovernmental eliminations. The LMP Project Office also created a process for creating one-time vendors in LMP without establishing compensating controls over that process. In addition, by not restricting the development of all business partner information to AESIP, Army managers have created significant internal control problems relating to the information within LMP. For example, the LMP Project Office created FSRs within LMP to create, update, and manage the vendor master table. As of March 2011, LMP activities had assigned FSRs to at least 133 LMP users that allowed them to edit or update vendor information to resolve contracting or payment problems. As the master data manager, only AESIP personnel should be able to create and manage vendor master data. Army ERP users should only have access to view vendor master data. Using a single Army-wide vendor master helps to provide the necessary internal control over the integrity and use of the vendor information. Army OBT and ASA(FM&C) should direct the Army ERP programs to cease developing system change requests to correct vendor master data within the individual ERP systems. The Army OBT and ASA(FM&C) should direct ERP managers to discontinue creating and using FSRs that allow users to create or update vendor master records and restrict that functionality solely to AESIP.

> *As of April 30, 2011, the ERP program managers spent or planned to spend about $1.3 million to derive unique vendor master tables.*

---

[22] This includes about $0.3 million that the GFEBS program manager intended to expend to develop vendor data within that system.

Developing a Way Forward

Based on our audit, the AESIP Program Manager took immediate actions to develop a temporary solution to provide TP1, TP2, and TP3 information to LMP until the Army develops a vendor master that fully complies with SFIS requirements. AESIP personnel stated that the General Services Administration would be consolidating eight of the Federal Procurement Systems and the Catalog of Federal Domestic Assistance databases, including CCR and FedReg, into the General Services Administration's System for Award Management database in May 2012. This consolidation effort will result in the development of a common vendor master within the Federal government and eliminate redundancies now contained in the FedReg and CCR databases. The new database will include data fields for the Trading Partner Indicator Codes and BPN Number that the AESIP vendor master can use to derive and populate a TP1 value. The concept of developing an integration program, such as AESIP, provides the Army a good control over the master data used in its ERP environment. The control of master data ensures the integrity of that data throughout the environment.

> *The concept of developing an integration program, such as AESIP, provides the Army a good control over the master data used in its ERP environment.*

Based on the General Services Administration's impending consolidation effort, the AESIP Program Manager should develop the vendor master based on the data structure intended for the System for Award Management database. The AESIP program manager should also establish data fields to populate the TP2 and TP3 domain values from the new database and derive and populate a TP1 domain value for each record based on these two domain values. The master vendor database should use the TP3 domain values as the key data field for controlling vendor records instead of the current CAGE code.

Conclusion

The Army had not developed the vendor master data needed to support the P2P business process. Instead, the Army managers allowed the LMP program manager to spend or plan to spend $1.3 million to create vendor tables. Although AESIP serves as the system integration program to provide common master vendor data for the Army ERP environment, it has not yet become the single source of authoritative reference data the Army needed to correctly establish and maintain business partner information. The efforts of the AESIP Program Management Office and the LMP program manager have not produced the vendor master data needed to eliminate the material weaknesses within the Army's P2P business process related to accounts payable and intragovernmental eliminations.

When transitioning to its ERP environment, Army OBT and ASA(FM&C) should have directed the AESIP program manager to develop common vendor master data that included the SFIS attributes needed to identify business partners for the P2P business process. This would have enabled the Army ERP systems to accurately classify, record, and report their Federal and non-Federal transactions. The Army OBT and ASA(FM&C) need to provide the AESIP program manager with the authority to function as the vendor master data manager and require AESIP to establish, maintain, and provide the correct business partner information to the Army ERP environment.

Considering that the System for Award Management database is scheduled to be available in May 2012, the AESIP should develop the ability to receive vendor master data from this new database.

Considering that the System for Award Management database is scheduled to be available in May 2012, the AESIP should develop the ability to receive vendor master data from this new database.

The Army OBT should ensure that the Army ERP systems have controls in place to prevent modifications of the AESIP vendor master data and the issuance of contracts and payments to business partners with inactive business partner registrations. To provide authoritative guidance to Army ERP program managers using vendor master data, the AESIP program manager must have visibility of the vendor master data source information to ensure AESIP is receiving all business partner information needed by the Army. In addition, the ASA(FM&C) should ensure that Army ERP program managers receive and use the vendor information in accordance with SFIS trading partner information requirements.

Recommendations, Management Comments, and Our Response

C.1. We recommend that the Deputy Chief Management Officer work with the Under Secretary of Defense (Comptroller) to review the use of legacy registration processes, such as Commercial and Government Entity Codes and Routing Identifier Codes, to determine whether DoD can eliminate the databases by incorporating them into the new System for Award Management database.

DCMO Comments

The DCMO agreed and stated that her office will work with the Under Secretary of Defense (Comptroller) and Defense Procurement Acquisition Policy to investigate the legacy vendor data registry process to determine whether DoD can eliminate the databases by incorporating them into the new System for Award Management database.

Our Response

The DCMO comments were responsive.

C.2. We recommend that the Director, Army Office of Business Transformation and Assistant Secretary of the Army (Financial Management and Comptroller) direct in policy that the:

a. Army Enterprise Systems Integration Program Manager serves as the vendor master data manager with the authority and personnel to:

(1) Require all systems doing business with the Army to use only the vendor master to populate business partner information.

(2) Prevent Army Enterprise Resource Planning system users from creating, modifying, or deleting vendor information and only allow for view access to master data by other system users.

(3) Validate the integrity of the business partner information contained in the vendor master records.

(4) Create all business partner records from information contained in the Federal Agency Registration and Central Contractor Registration until the System for Award Management Database comes on line.

(5) Establish individual business partner records using the Business Partner Network number and create data files to populate the applicable Standard Financial Information Structure attributes.

(6) Issue instructions on the administration and use of Army vendor information.

Department of the Army Comments

The ASA(FM&C), responding on behalf of the Army, agreed and stated that the Army Business System Information Technology Strategy states that AESIP synchronizes and syndicates select enterprise master data applicable to each Army ERP system. The ASA(FM&C) also stated that the Army will continue to leverage its business system information technology strategy and governance procedures to implement additional improvements as updates and opportunities avail themselves. The Army Business System Information Technology Strategy, as a living document, serves as the Army's foundation and roadmap for executing the Army enterprise architecture and will evolve in response to changes. Consequently, AMC and ASA(FM&C) personnel will work with OBT personnel to reevaluate and adjust as necessary the functions of the AESIP program manager and his role as the vendor master data manager.

Our Response

The ASA(FM&C) comments were partially responsive. The ASA(FM&C) stated that AMC and ASA(FM&C) personnel will work with OBT personnel to reevaluate and adjust as necessary the functions of the AESIP program manager and his role as the vendor master data manager. However, she did not identify how the AESIP program manager will implement the six sub elements of the recommendation. We request that the ASA(FM&C) and Director, Army OBT, reevaluate their response to this recommendation and provide additional comments on the final report, detailing how they plan to provide the AESIP program manager with the authority and personnel to take the recommended actions.

b. Army and non-Army Routing Identifier Code locations register within the Federal Agency Registration database before creating a business partner record in the Army vendor master record for doing business transactions with the Army or accepting any supplemental business partner information from those locations.

Department of the Army Comments

The ASA(FM&C), responding on behalf of the Army, agreed.

Our Response

The Army comments were nonresponsive. The Army comments did not specifically address the policy needed to ensure that Army and non-Army Routing Identifier Code locations register within Federal Agency Registration database before creating a Army vendor master record for doing business transactions with the Army or accepting any supplemental business partner information from those locations. We request the Director, Army OBT and the ASA(FM&C) reconsider their response to this recommendation and provide additional comments on the final report, detailing how they enforce require the Army Routing Identifier Code locations to register in the Federal Agency Registration or System for Award Management database before establishing a vendor record in AESIP.

c. Army Enterprise Resource Planning Project Offices:

(1) remove functional security roles capable of adding, revising, or deleting vender information; and

(2) cease developing change requests for correcting of vendor master data.

Department of the Army Comments

The ASA(FM&C), responding on behalf of the Army, agreed.

Our Response

The Army comments were nonresponsive. The ASA(FM&C) did not specifically address the plan to direct the Army ERP Project Offices to remove FSRs capable of adding, revising, or deleting vendor information from the ERP systems and cease developing change requests for correcting vendor master data outside the AESIP environment. The ASA(FM&C) needs to address how the Army plans to limit the responsibility of Army ERP Project Offices in managing the master vendor data. We request that the Director, Army OBT, and the ASA(FM&C) reconsider their response to this recommendation and provide additional comments on the final report, detailing how the Army will limit the ability of Army ERP Project Offices from changing vendor master data and ensure that only the AESIP program manager has the authority, access, and funding needed to update vendor information.

C.3. We recommend that the Army Enterprise Systems Integration Program Manager create and manage a vendor master based on the System for Award Management database that can:

a. Populate required vendor-related Standard Financial Information Structure attributes with valid domain values.

b. Establish the Business Partner Network number as the key data field for all business partner records and use that data field when receiving and sending information to Army and other systems.

c. Identify and track the business partner registration status in the Central Contractor Registration and Federal Agency Registration databases and System for Award Management database once implemented.

d. Obtain all vendor information needed by Army Enterprise Resource Planning systems and supporting systems.

Department of the Army Comments

The ASA(FM&C), responding on behalf of the Army, agreed and stated that the AESIP program manager will work with the stakeholders to implement this recommendation. Actions taken will require policy, system, and process changes, and validation of Army vendor data to ensure that the Army vendor master is in accord with System for Award Management vendor data.

With the respect to System for Award Management, the ASA(FM&C) stated that according to the latest data element listing from the General Services Administration, the term Business Partner Number will not be used. Commercial and non-government entities will register with their Data Universal Numbering System number and it will be stored in the Data Universal Numbering System number field. DoD agencies will register their DODAAC and it will be stored in the DODAAC field. She stated that the AESIP vendor master will be enhanced to be in line with the new data and that Army managers will work with LMP on the best and most cost effective approach to have their system support the new design. The ASA(FM&C) stated that the Army had completed actions related to Recommendation C.3.c. AESIP currently receives the registration status and passes this information to the Army ERPs and will continue to receive and provide this information with the migration to System for Award Management. The ASA(FM&C) also stated that performing all derivations in AESIP, syndicating the results to other systems, and prohibiting changes anywhere except in AESIP is the desired goal. However, a cost-benefit analysis will be required to determine if this yields a tangible return on investment.

Our Response

The Army comments were responsive. Although the new System for Award Management may not use the term Business Partner Number, the Data Universal Numbering System number and DoDAAC contain the exact data that the Army will require to correctly establish the SFIS business partner number (TP3) domain values. Therefore, the AESIP Program Management Office must ensure that it develops a methodology to populate the SFIS TP3 values using both the Data Universal Numbering System number and DoDAAC and use the TP3 element as the primary key for establishing records in the AESIP vendor tables.

C.4. We recommend that the Assistant Secretary of the Army (Financial Management and Comptroller) validate that the Logistics Modernization Program system has controls in place to reject new contracts and payment requests from business partners with inactive vendor registration flags.

Department of the Army Comments

The ASA(FM&C), responding on behalf of the Army, agreed and stated that the Army will validate transactional data as part of internal control assessment. The test will include a validation of business partner data in LMP compared to the data in AESIP. This validation will occur after the Army has implemented System for Award Management, but not later than September 30, 2012.

Our Response

The Army comments were responsive.

Appendix A. Scope and Methodology

We conducted this performance audit from August 2010 through January 2012 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

During this audit, we received detailed briefings from the BTA on the P2P business process available within commercial software and from the LMP Project Office on how Army managers had implemented the software to conduct and report Army business events. We conducted site visits to the LCMC, the Depot, and DFAS Columbus to understand how each activity used LMP to perform the P2P business process and control system access. We also held detailed discussions with personnel from the offices of the USD(C); ASA(FM&C); AESIP PM; and AMC G3/5, G6, and G8; as well as within the Army OBT and DFAS.

We obtained documentation to support Army's implementation of the P2P business process and initiatives to address abnormal accounts payable balances, local vendor pay, and prevalidation. We obtained a database of the 2.3 million business partners in the LMP vendor table as of January 4, 2011, and assessed anomalies in the database. We also obtained the LMP disbursement file for "Delivered Orders - Obligations Paid," (GLAC 4902) for November 2010 and reconciled it to the amounts reported on the monthly unadjusted trial balances for AWCF activities using LMP. We sorted the 83,894 transactions in the file to identify those transactions with a commitment number that would have affected the P2P business process. This left us with a population of 57,330 transactions. We provided the adjusted file to the statisticians in the Quantitative Methods and Analysis Division, DoD Office of Inspector General. After removing the transactions under one thousand dollars and stratifying the remaining transactions into four strata, the statisticians selected a stratified random attribute sample of 120 transactions. For each of the 120 transactions, we reviewed documentation to assess the propriety of the transaction and the validity of the LMP audit trail.

We analyzed the unadjusted trial balances reported by LMP activities for the fiscal years ended September 2008, 2009, and 2010 and for the first six months of FY 2011. We assessed the number and dollar values of abnormal balances reported in 2 proprietary and 12 budgetary general ledger accounts supporting the P2P business process. We also assessed the abnormal account balances within GLAC 4450, GLAC 4610, and GLAC 4700, supporting the AWCF's unobligated balance as of September 30, 2010, and the first 3 months and August of FY 2011.

We used statistical sampling and other analytical procedures to assess how UAM administrators and LMP user's supervisors at the LCMC and the Depot controlled system access and assigned FSRs to users. We obtained the LMP system access assigned to all personnel in the LCMC and the Depot as of October and November 2010 and assessed whether the issuance of user access met the NIST requirements for account management, segregation of duties, and least privilege access. We queried individuals having LMP access using a survey we developed. See Appendix G for details on sample methodology and results.

Use of Computer-Processed Data

To perform this audit, we obtained data from LMP. We determined data reliability by reviewing selected P2P business transactions and the support for them. We reviewed the month-end LMP trial balances from September 2010 through March 2011 and August 2011. We determined the propriety of the balances reported by LMP activities for the GLACs supporting the P2P business process through reviews of the posting logic for the underlying business events. In the accounts reviewed, several LMP activities reported abnormal balances and differences existed between associated proprietary and budgetary general ledger accounts. We also obtained an LMP disbursement file (GLAC 4902) for November 2010, and we were able to validate the balance to the November 2010 LMP trial balances reported by the LMP activities. We reviewed disbursement vouchers and supporting documentation for 96 of 120 sampled transactions. Our review of the documentation showed that LMP did not always accurately record data related to the P2P process. We relied on the source documents to provide us with the actual dates, document numbers, and amounts that LMP activities should have recorded in LMP. LMP posting logic problems caused abnormal balances and the incomplete and inaccurate posting of business events adversely affected the reliability of the LMP reported data.

We also reviewed the 2.3 million vendor records in LMP as of January 4, 2011, and user access databases for the two LMP activities we visited. Through our review of information associated with the vendor records and FSRs assigned to users, we determined that the LMP vendor records did not accurately classify business partners but LMP accurately reflected user access privileges. However, LMP system access assigned to users did not always reflect the access that UAM administrators and user's supervisors believed users possessed. Our assessment indicated that the LMP data were sufficient for reaching audit conclusions. However, the findings in the report address the computer-processed data weaknesses found and the needed corrective actions.

Use of Technical Assistance

The Quantitative Methods and Analysis Division provided technical assistance throughout the sample selection and evaluation process. The Quantitative Methods and Analysis Division provided a stratified sample of disbursements made by LMP in November 2010 and a statistical sample of LMP user access at the Depot as of November 1, 2010. See Appendix G for the statistical sampling methodology.

Appendix B. Prior Coverage

During the last five years, the GAO, DoD IG, and the U.S. Army Audit Agency have issued 10 reports discussing LMP functionality. Unrestricted GAO reports can be accessed over the Internet at http://www.gao.gov. Unrestricted DoD IG reports can be accessed at http://www.dodig.mil/audit/reports. Unrestricted U.S. Army Audit Agency reports can be accessed from .mil and gao.gov domains over the Internet at https://www.aaa.army.mil/.

GAO

GAO Report No. 11-53, "Defense Logistics: Improved Management Oversight of Business Systems Modernization Efforts Needed," October 7, 2010

GAO Report No. 10-461, "Defense Logistics: Actions Needed to Improve Implementation of the Army Logistics Modernization Program," April 30, 2010

GAO Report No. 09-852R, "Defense Logistics: Observations on Army's Implementation of the Logistics Modernization Program," July 8, 2009

GAO Report No. 07-860, "DoD Business Transformation: Lack of an Integrated Strategy Puts the Army's Asset Visibility System Investments at Risk," July 27, 2007

DoD IG

DoD IG Report No. D-2011-15, "Insufficient Governance Over Logistics Modernization Program System Development," November 2, 2010

DoD IG Report No. D-2009-87, "Controls Over Contract Obligation Data in the Logistics Modernization Program," June 15, 2009

DoD IG Report No. D-2007-065, "Controls Over the Prevalidation of DOD Commercial Payments," March 2, 2007

Army

U.S. Army Audit Agency Report No. A-2007-0205-FFM, "Logistics Modernization Program System Federal Financial Management Improvement Act of 1996 Compliance–First Deployment Functionality," September 7, 2007

U.S. Army Audit Agency Report No. A-2007-0163-FFM, "FY 03–FY 05 Obligations Recorded in the Logistics Modernization Program," July 27, 2007

U.S. Army Audit Agency Report No. A-2007-0154-ALR, "Follow up Audit of Aged Accounts–U.S. Army Communications-Electronics Life Cycle Management Command," July 2, 2007

Appendix C. Description of Technical Requirements and Standards

This appendix describes the National Institute of Standards and Technology (NIST) standards reviewed, the five standards of internal control, the three material weaknesses related to the LMP P2P business process, and the Statement of Federal Financial Accounting Standard related to Accounts Payable.

NIST Standards

- **Account Management** requires entities to establish account management controls. An entity should have the ability to: identify authorized system users and specify user access privileges; require appropriate approvals for establishing accounts; establish, activate, modify, disable, and remove accounts; notify account managers when users are terminated or transferred; deactivate accounts of terminated or transferred users; grant access to the system based on a valid access authorization, the intended system usage, and other attributes as required by the organization or associated missions/business functions; and review accounts in accordance with the organizationally defined frequency.

- **Separation of Duties** requires management to segregate system access so that more than one person is required to complete an end-to-end process using assigned access authorizations. Segregation of duties helps prevent and detect user errors and mitigate the potential for fraud and misuse of assets. The GAO internal control standards refer to this as segregation of duties. Within the report, we refer to this as segregation of duties.

- **Least Privilege** requires system managers to assign user authority in such a manner so that only the information and resources necessary for legitimate purposes can be accessed. Least privilege requires that activities assign user access based upon the minimum access that a user requires when performing the tasks assigned by business function and organization.

Standards of Internal Control

- **Control Activities** are the policies, procedures, and mechanisms in place to meet agency objectives, including proper segregation of duties, physical controls over assets, proper authorization, and appropriate documentation. Entities should also design application controls to ensure that the ERP systems can authorize and process transactions accurately.

- **Control Environment** includes the organizational structure and culture to sustain organizational support for effective internal control. Management must clearly demonstrate its commitment to competence in the workplace when designing, evaluating, or modifying the organizational structure. Management must clearly define areas of authority and responsibility and appropriately delegate the authority and responsibility throughout the agency. Management must also establish a suitable hierarchy for

reporting and uphold the need for personnel to possess and maintain the proper knowledge and skills to perform their assigned duties as well as understand the importance of maintaining effective internal control within the organization. Management's philosophy for establishing and maintaining effective internal control should aid in the successful implementation of internal control systems.

- **Information and Communications** requires management to communicate relevant, reliable, and timely information to personnel at all organization levels. It is also crucial that an agency communicate with outside organizations whether providing information or receiving it. Situations requiring effective communications of information include receiving updated guidance from central oversight agencies, management communicating requirements to the operational staff, and operational staff communicating with the information systems staff to modify application software to extract data requested in the guidance.

- **Monitoring** requires management to scrutinize the effectiveness of internal control in the normal course of business, including thorough periodic reviews and reconciliations or comparisons of data. Management should integrate periodic assessments in the agency's operations. All personnel should report deficiencies found in internal control to the appropriate personnel and management responsible for that area and they should evaluate and correct the deficiencies.

- **Risk Assessment** involves identifying internal and external risks that may prevent the organization from meeting its objectives. When identifying risks, management should take into account relevant interactions within the organization as well as with outside organizations and analyze the potential effect or impact on the agency.

Material Weakness Description

Office of Management and Budget Circular No. A-123 defines a material weakness as a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. The material weaknesses discussed in this report are:

- Accounts Payable. The Army relies on unsupported adjustments processed by DFAS to report accounts payable balances. These adjustments were required to account for undistributed disbursements and intragovernmental accounts payable. Army is working on implementing an upgrade for constructive receipts in LMP that targets correction of the accounts payable accounting and reporting issues. The LMP upgrade is scheduled for December 2011. Additional steps that will solidify correction of this weakness include actions to clean up legacy balances, elimination of record data types, correction of trading partner data, and full usage of Wide Area WorkFlow.

- Abnormal Account Balances. In FY 2010, the AWCF Industrial Operations and Supply Management activities (limit-level) reported 81 abnormal account balances, valued at $2.1 billion, including 33 accounts for $1.6 billion in the LMP environment. The

abnormal balances in LMP are caused by incorrect general ledger attributes. Full implementation of the SFIS in LMP will correct the abnormal balances caused by incorrect general ledger attributes. The remaining abnormal balances will be manually reconciled and corrected.

- Intragovernmental Eliminations. Army systems were unable to collect, exchange, and reconcile buyer and seller intragovernmental transactions, resulting in adjustments that were not verifiable. DoD and AWCF systems did not capture the trading partner financial data at the transaction level needed to facilitate reconciling and eliminating intragovernmental transactions. DoD procedures require that the Army adjust its buyer-side transaction data to agree with seller-side transaction data from other Government entities without the entities performing proper reconciliations. As a result, DFAS Indianapolis adjusted to AWCF accounts to force the accounts to agree with the corresponding records of intragovernmental trading partners.

Defining Accounts Payable

Statement of Federal Financial Accounting Standards Number 1, "Accounting for Selected Assets and Liabilities," March 30, 1993, states the following about accounts payable:

- Accounts payable represent amounts owed by a Federal entity for goods and services received from the entities; progress in contract performance and rents due to other entities.

- The amounts owed for goods or services received from Federal entities represent intragovernmental transactions and require separate reporting from amounts owed to the public.

DoD FMR, volume 4, chapter 9, "Accounts Payable," August 2009, requires DoD systems to record accounts payable transactions using the appropriate U.S. Government Standard General Ledger proprietary and budgetary accounts as defined in SFIS.

Appendix D. Acronyms and Abbreviations

AESIP	Army Enterprise Systems Integration Program
AMC	Army Materiel Command
ASA(FM&C)	Assistant Secretary of the Army (Financial Management and Comptroller)
AWCF	Army Working Capital Fund
BEA	Business Enterprise Architecture
BPN	Business Partner Network
BTA	Business Transformation Agency
CAGE	Commercial Activity Government Entity
CCR	Central Contractor Registration
DCMO	Deputy Chief Management Officer
DFAS	Defense Finance and Accounting Service
DoDAAC	DoD Address Activity Code
DoD FMR	DoD Financial Management Regulation
DoD IG	DoD Inspector General
ERP	Enterprise Resource Planning
FISMA	Federal Information Security Management Act of 2002
FSR	Functional Security Role
GAO	Government Accountability Office
GFEBS	General Fund Enterprise Business System
GLAC	General Ledger Account Code
LCMC	Life Cycle Management Command
LMP	Logistics Modernization Program system
MIPR	Military Interdepartmental Purchase Request
NIST	National Institute of Standards and Technology
OBT	Office of Business Transformation
P2P	Procure-to-Pay
SFIS	Standard Financial Information Structure
UAM	User Account Management

Appendix E. Business Transformation Agency Procure-to-Pay Illustration

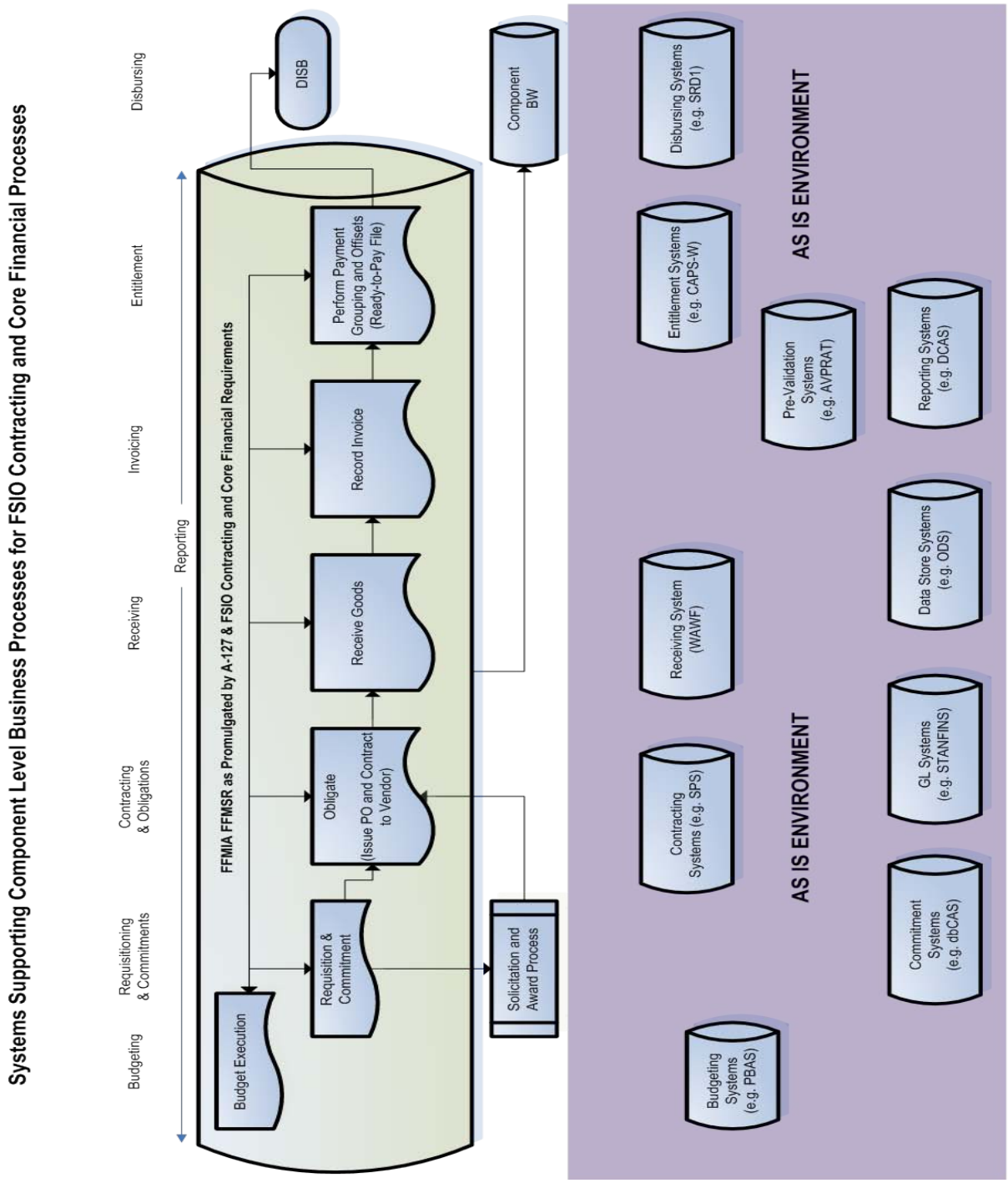
BEA 7.0 describes the P2P business process as encompassing all business functions necessary to obtain goods and services. The BEA P2P business process identifies six phases during which activities post financial transactions: Requisitioning and Commitments, Contracting and Obligations, Goods Receipt, Invoicing, Entitlement, and Disbursing. The illustration in Figure E-2, which BTA provided in August 2010, compares the intended BEA business process (top portion) with the current "As Is" environment (bottom portion). The process also had a phase entitled "budgeting" which we will assess during a separate audit of the LMP budget process. Figure E-1 defines the acronyms used in Figure E-2.

Figure E-1. Listing of Illustration Acronyms

AVPRAT – Accounting Vendor Pay and Analysis Tool
BW - Business Warehouse
CAPS-W – Computerized Accounts Payable System- Windows
dbCAS – Database Commitment Accounting System
DCAS – DoD Cash Accountability System
FFMIA – Federal Financial Management Improvement Act
FFMRS – Federal Financial Management System Requirements
FSIO – Financial Systems Integration Office
ODS – Operational Data Store
PBAS – Program Budget and Accounting System
SPS – Standard Procurement System
SRD-1 – Standard Finance System Redesign
STANFINS – Standard Financial System
WAWF – Wide Area WorkFlow

Source: Auditor Developed

Figure E-2. Business Transformation Agency Procure-to-Pay Illustration



Source: Business Transformation Agency

Appendix F. Segregation of Duties

NIST Special Publication 800-53, Revision 3, "Recommended Security Controls for Federal Information Systems and Organizations," May 2010, control AC-5, defines segregation of duties as the system access control that requires more than one person to complete an end-to-end process using assigned access authorizations. Segregation of duties requirements applicable to the development of LMP FSRs were:

- segregate duties of individuals as necessary to prevent malicious activity without collusion,
- document segregation of duties risk by the organization, and
- implement segregation of duties through assigned information system access authorizations.

According to industry best practices, the best way to minimize the opportunity to commit fraud is to implement a good system of internal controls, which includes proper authorizations and segregation of duties. Within the P2P business process, the same user should not perform more than one of the following functions: purchasing, receipt of goods, recording of invoices, modification of inventory records, and creating or updating the master tables.

Identifying Potential Segregation of Duty Conflicts

Table F-1 shows the LMP transaction screens assignable to FSRs within the five P2P functions.

Table F-1. LMP Transaction Screens for Procure-to-Pay Process

Purchasing	Receipt of Goods	Recording of Invoices	Modify Inventory Records	Master Tables
FMY1 – Create Funds Commitment	MB1B – Goods Movement	FBR2 – Post Document	HUNINV05 – Clears Inventory Differences	MM01 – Create Material
FMY2 – Change Funds Commitment	MB1C – Other Goods Receipt	FB02 – Change an Invoice	LI11N – Enter Inventory Count	MM02 – Change Material
FMZ1 – Create Funds Obligation	MIGO – Goods Movement (Receipt)	FB60 – AP Invoicing	LI12N – Change Inventory Count	MM06 – Flag for Deletion
FMZ2 – Change Funds Obligation	ZIGO – Goods Receipt	FB65 – A/P Credit Memo	LI20 – Clear Inventory Differences	MM17 – Mass Change Material Master

Table F-1. LMP Transaction Screens for Procure-to-Pay Process
(Continued)

Purchasing	Receipt of Goods	Recording of Invoices	Modify Inventory Records	Master Tables
ME21N – Create Purchase Order		F-47 – Down Payments	LI21 – Clear Inventory Difference in MMI	XK01 – Create Vendor Master (All Areas)
ME22N – Change Purchase Order		MIRO – Post Invoice	MB1A – Goods Issue	XK02 – Change Vendor Master
ME29N – Release Purchase Order			MB11 – Goods/Inventory Adjustment	ZAOR – ZPS_Recovery Table Maintenance
ME51N – Create Purchase Requisition			MI07 – Post Cycle Count Differences	ZFUNDK2 – Maintain Funding Table
ME52N – Change Purchase Requisition			MR11 – Goods/Invoices Receipts Adjustment	ZPSCFNDK – Maintain Master Tables
ME53N – View Purchase Request			MR11SHOW – Reverses Good/Invoice Receipts Adjustments	
ME59 – Auto Generation of Purchase Order			MR21 – Pricing Changes	
ZMILS – Process Requirement			MSC2N – Change Material Batch	
ZMMR – Mass Create Vendor Returns			VA01 – Create Sales Order	
ZMO – Interfaces-Purchasing Interface Monitor			VA02 – Change Sales Order	
ZFUND – Funds Certification Process				

Using the NIST guidance and various publications from major accounting firms, we identified that access to the following LMP transaction screens could pose segregation of duties conflicts when given to a single user.

- The individual initiating or modifying a purchase request should not be able to create (XK01) or modify the vendor record (XK02), record invoices (FB60, MIRO), receive goods and services (MIGO, ZIGO), or reconcile inventory records (MB11).

- The individual creating or approving purchase orders (ME21N, ME22N) should not be able to record invoices (FB60, MIRO).

- The individual receiving goods and services (MIGO, ZIGO) should not have purchasing functions (ME21N, ME22N, ME51N, ME52N) or be able to modify the vendor records (XK01, XK02) or record invoices (MIRO, FB60) or credit memos (FB65).

The individual performing the three-way match of obligations, invoice, and receiving reports (FB60, MIRO) should not also be involved in receipt functions (MIGO, ZIGO) or purchasing functions (ME21N, ME22N, ME51N, ME52N), modify the vendor record (XK01, XK02), or have any inventory functions (transaction screens listed under Modify Inventory Records in Table F-1).

Appendix G. Statistical Sampling Methodology

Based on the results of our judgmental review of system access at the LCMC, we worked with the Quantitative Methods and Analysis Division to design a statistical sample at the Depot to assess system access.

Sampling Purpose

The purpose of the statistical sampling plan was to determine whether system access provided to users at the Depot demonstrated proper implementation of the FISMA requirements related to segregation of duties, least privilege, and account management.

Universe Represented

We obtained the universe of LMP users assigned to the Depot as of November 1, 2010. The universe consisted of 943 users. We identified the specific FSRs each user held. The number of FSRs held by users ranged from 2 to 95.

Sampling Design

The sampling design was a stratified variable sample consisting of two strata: a census stratum and a random stratum. For the census stratum, we selected the 13 users who had the highest combined number of restricted FSRs and total FSRs assigned to them. For the random stratum, we randomly selected without replacement 65 users from the remaining users in the universe. We randomly selected users using the =RAND() function in Excel 2007.

Sampling Methodology

To determine whether the Depot had implemented effective account management practices and help us determine potential segregation of duties and least privilege conflicts, we developed a questionnaire containing three questions. We performed face-to-face interviews while at the Depot with 11 of the 78 LMP users. Seven of the 13 users were from the census stratum and 4 of the 65 users from the random stratum. We then designed and administered an e-mail survey and transmitted it to the remaining 67 LMP users. The e-mail survey asked the users to identify their job titles and provide information about the FSRs assigned, the tasks they performed on a regular basis, and any FSRs and responsibilities assigned previously related to LMP. In the e-mail survey, we provided a spreadsheet listing the FSRs assigned to each sampled user as of November 1, 2010, including the transaction screens assigned within each FSR. We asked the respondents to identify the purpose of each FSR assigned, the use of transaction screens within each FSR, and the functions they accomplished using the transaction screens. We also requested that the user identify any assigned FSRs they did not use. We asked these questions to determine the extent to which the respondent used their access and determine whether the FSRs potentially caused segregation of duties or least privilege conflicts and whether the Depot followed proper account management practices. We also asked if they were part of the LMP Transition Team to determine if that could be cause for assigned access outside of a respondent's normal duties. We used responses to the questionnaire to answer the following four questions.

1. Was the user aware of the FSRs assigned? For this attribute, we assigned:

    - "No" to definitive statements made by respondents that indicated that they were not aware of the FSRs assigned, such as "There is no way I have this many FSRs," "Can't you send me the FSRs I really have," or "I have never used LMP."

    - "Yes" when the respondent provided a clear explanation of how they used at least one of the transaction screens assigned within each FSR.

    - "Not determinable" for respondents who did not provide a clear response to the question.

2. Does the user have the FSRs needed to perform job? For this attribute, we assigned:

    - "No" to the one respondent who stated that she could use additional screens not assigned.

    - "Yes" to respondents who stated they had the FSRs needed to perform their jobs.

    - "Not determinable" to the three respondents who had departed the Depot before we administrated the survey.

3. Does the user have excess FSRs assigned? For this attribute, we assigned:

    - "No" to respondents who identified all the FSRs assigned and the transaction screens they used within the FSRs. We also assigned a "No" to the one respondent who stated that she could use additional screens not assigned.

    - "Yes" to respondents who stated they did not use LMP, one or more assigned FSRs, or who could not identify all the FSRs assigned and the transaction screens they used.

4. Does potential exist for a segregation of duties conflict within the P2P business process? Using the information within Appendix F, we assessed the FSRs and transaction screens assigned to each of the 78 LMP users. For the attribute, we assigned:

    - "No" if a user's access to a combination of LMP screens did not allow the user to accomplish more than one function (authorization, execution, custody, or recording), we determined that no potential segregation of duties conflict existed.

    - "Yes" if a user's access to a combination of LMP screens allowed the user to accomplish more than one function (authorization, execution, custody, or recording), we determined that a potential existed for a segregation of duties conflict.

Sampling Results

Table G-1 shows how we categorized the responses from the 78 sampled LMP users. We provided the results to the Quantitative Methods and Analysis Division for statistical projection.

Table G-1. User Access Assessment

Attributes Assessed	Yes	No	Not Determinable
1. Is the user aware of the FSRs assigned?	10	32	36
2. Does the user have the FSRs needed to perform the user's job?	74	1	3
3. Does the user have excess FSRs assigned (FSRs that they do not use)?	73	5	0
4. Within the assigned FSRs, is there a potential segregation of duties conflict?	20	58	0

A significant number of users were unaware of the access assigned (attribute 1, "No" response). Most users believed that had the access they needed to perform their job (attribute 2, "Yes" response). In addition, most users had access to transaction screens they did not require to perform their job (attribute 3, "Yes" response) or had FSRs assigned or transaction screens that potentially resulted in a segregation of duties conflict (attribute 4, "Yes" response). Table G-2 provides the statistical estimate of the 943 users for each of the four attributes at a 90 percent confidence level.

Table G-2. User Access Attribute Projections
(90 Percent Confidence Level)

Attributes Assessed	Lower Bound	Point Estimate	Upper Bound
1. Users unaware of FSRs assigned	289	391	494
2. Users who believed they had the access needed to do their job	830	886	942
3. Users who had at least one FSR assigned that was not used	829	885	941
4. Users with potential segregation of duties conflict	64	140	215

We concluded that the Depot had not effectively implemented the requirements for accounts management, segregation of duties, and least privilege.

Appendix H. Developing the Vendor Master Using Standard Financial Information Structure Attributes

The SFIS business rules require ERP systems to use SFIS attribute fields for general ledger posting and financial reporting. The BPN number is the key for obtaining and reporting business partner information and used for establishing a vendor master record. Information extracted from either the FedReg or CCR should be used to create all records and populate the three SFIS Trading Partner Information attributes. Table H-1 shows how AESIP personnel should obtain the attributes and domain values from the data reported in the source files (FedReg and CCR) and create the master vendor data in AESIP.

Table H-1. SFIS to AESIP Attributes and Domain Values

SFIS			Source Data Field		AESIP	
Attribute	**Domain Value**	**Entity**	**FedReg**	**CCR**	**Data Field**	**Domain Value**
TP1	F	Federal Trading Partner	Data field not available	Type of Organization field identified as Federal	Federal/ Non-Federal Indicator	F
	N	Non-Federal Business Partners	N/A	Type of Organization field identified as other than Federal		N
TP2	3-digit code	Federal Trading Partner	Department Code	N/A	Trading Partner Indicator Code	Department Regular Code
TP3	Data Universal Numbering System number	Non-DoD Federal and Private Businesses	BPN Number	Data Universal Numbering System number	BPN Number	Data Universal Numbering System number
	DoD Plus DoDAAC	DoD	BPN Number	Data Universal Numbering System Number		DoD Plus DoDAAC

Trading Partner Attribute Requirements

The SFIS established three distinct attributes that systems must record at the transaction level for general ledger accounts that identify the business partners involved. These attributes allow

accounting systems to identify intragovernmental transactions for use during the elimination process when developing consolidated financial statements.

- The SFIS Federal/Non-Federal Indicator (TP1) attribute identifies the type of business partner involved in a transaction. The type of business partner involved in a transaction determines whether to report the transaction as Federal or non-Federal. To identify intragovernmental transactions for elimination, the Army ERP systems need to have the capability to distinguish between Federal and non-Federal transactions. To develop SFIS attributes, AESIP personnel need to establish each business partner's TP1 information using data obtained directly from the CCR data field that identified the type of organization the business partner registered as or record a domain value of "F" for all business partners registered in FedReg.

- The SFIS Trading Partner Indicator Code (TP2) attribute identifies the Department Regular Code of the other Federal entity involved in a transaction.[23] The TP2 attribute allowed Army ERP managers to identify the specific Federal entities involved in intragovernmental transactions for use in its intragovernmental elimination process. For Federal business partners, AESIP personnel need to establish each business partner's TP2 information using data obtained from the FedReg's Department Regular Code data field. For non-Federal business partners, the TP2 domain value is blank.

- The SFIS BPN Number (TP3) attribute records a unique, nine-position alphanumeric that identifies business entities on a location-specific basis. To populate the domain value, AESIP personnel need to establish each business partner's TP3 information by obtaining the DUNS number or "DoD" plus DoDAAC directly from FedReg or CCR. The TP3 attribute should be the primary data field for establishing the AESIP vendor master records.

Business Partner Status

Army ERP systems also needed to have the capability to identify the current registration status for each business partner. The Federal Acquisition Regulation does not allow inactive business partners from receiving new contracts or additional payments until a valid registration exists. The CCR and FedReg provide the registration status of business partners. AESIP personnel recorded this status in a data field and had to ensure that the vendor master identified the current registration status of each business partner and passed that information to ERP systems regularly.

[23] The Department of the Treasury assigned a Department Regular Code to each Federal entity. For example, the Department Regular Code for the Army is "021."

Glossary

Attributes - characteristics of a U.S. Government Standard General Ledger account captured and used to meet specific reporting requirements. Agency systems must record transactions using U.S. Government Standard General Ledger 4-digit accounts plus attributes in order to capture information needed to meet external reporting requirements.

Business Rules - principles identified in a DoD BEA document that should be followed so that the target accounting system is populated with the correct data.

Commercial and Government Entity (CAGE) Code – a 5-digit identification number used extensively within the Federal Government to identify companies doing or desiring to do business with the Federal Government. The CAGE code provides a standardized method of identifying a given facility at a specific location.

Data Universal Numbering System Number – unique 9-digit number that non-government entities and Federal civilian entities (non-DoD) must obtain from Dun & Bradstreet, Incorporated. An entity must use the number as its BPN number and for Federal Agency Registration and CCR.

DoD Activity Address Code (DoDAAC) – a unique identifier of a unit, activity, or organization that has the authority to requisition and/or receive materiel. DoD entities must use the letters "DOD" followed by their 6-digit DoDAAC (for example, DOD123456) as their BPN number.

Domain Values – the possible valid data elements within an attribute. For example, the Federal and Non-Federal Indicator use an "F" domain value to classify a transaction as Federal and an "N" domain value to classify a transaction as Non-Federal.

Deputy Chief Management Officer Comments

DEPUTY CHIEF MANAGEMENT OFFICER
9010 DEFENSE PENTAGON
WASHINGTON, DC 20301-9010

FEB 18 2012

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL (FINANCIAL MANAGEMENT AND REPORTING)

SUBJECT: Comments to Draft Audit Report, "Logistics Modernization Program System Procure-to-Pay Process Did Not Correct Material Weaknesses" (Project No. D2010- D000FI-0234.000)

This memorandum responds to your request for comments on one audit recommendation contained in the draft audit report issued January 3, 2012. We concur with the recommendation contained in the subject draft audit report. Our detailed response to the recommendation is provided in the attachment.

[redacted] is the point of contact for this response. He can be reached by telephone at [redacted] or by email at [redacted]

Elizabeth A. McGrath

Attachment:
As stated

**DEPARTMENT OF DEFENSE OFFICE OF THE INSPECTOR GENERAL (DoDIG)
DRAFT REPORT DATED JANUARY 3, 2012, PROJECT NO. D2010-D000FI-0234.000
"LOGISTICS MODERNIZATION PROGRAM SYSTEM PROCURE-TO-PAY
PROCESS DID NOT CORRECT MATERIAL WEAKNESSES"**

**OFFICE OF THE DEPUTY CHIEF MANAGEMENT OFFICER (DCMO)
COMMENTS TO DODIG RECOMMENDATION**

RECOMMENDATION C.1: "We recommend that the Deputy Chief Management Officer work with the Under Secretary of Defense (Comptroller) to review the use of legacy registration processes, such as Commercial and Government Entity Codes and Routing Identifier Codes, to determine whether DoD can eliminate the databases by incorporating them into the new System for Award Management database."

DCMO RESPONSE: Concur. The Deputy Chief Management Officer will work with the Under Secretary of Defense (Comptroller) and Defense Procurement Acquisition Policy to investigate the legacy vendor data registry process to determine whether DoD can eliminate the databases by incorporating them into the new System for Award Management database.

Department Of The Army Comments

DEPARTMENT OF THE ARMY
OFFICE OF THE ASSISTANT SECRETARY OF THE ARMY
FINANCIAL MANAGEMENT AND COMPTROLLER
109 ARMY PENTAGON
WASHINGTON DC 20310-0109

REPLY TO
ATTENTION OF

FEB 2 2012

SAFM-ZA

MEMORANDUM FOR Assistant Inspector General for Audit, Department of Defense Inspector General, 4800 Mark Center Drive, Alexandria, VA 22350-1500

SUBJECT: Army Response to Draft Report Project No. D2010-D000FI-0234.000, Logistics Modernization Program System Procure-to-Pay Process Did Not Correct Material Weaknesses

1. Enclosed is our response to recommendations A, B, and C in the subject draft report. The draft report recommends the Army develop a plan of action and milestones to bring the Logistics Modernization Program (LMP) system into compliance with the DoD Business Enterprise Architecture (BEA) Procure-to-Pay (P2P) business rules. We agree that the current P2P process has too many functions residing outside of LMP and that increased integration of these functions is desirable. We will review the feasibility of increasing the level of P2P integration within LMP. Results of the review will inform a plan of action and milestones (POAM) identifying the desirable level of P2P integration within LMP.

2. The report recommends the Army develop a plan to improve system access controls within LMP. As part of audit readiness discovery and evaluation activities, we will assess LMP key controls, identify deficient areas, and develop a plan to resolve identified deficiencies.

3. The report also recommends that we direct in policy that the Army Enterprise Systems Integration (AESIP) Program Manager (PM) serve as the vendor master data manager. We concur with the current role of the AESIP PM as vendor master data manager.

4. My point of contact for this action is [redacted]. She can be reached by e-mail at [redacted] or by telephone at [redacted].

Encl

For Mary Sally Matiella, CPA

Printed on Recycled Paper

Enclosure: Official Comments

Logistics Modernization Program System Procure-to-Pay Process
Did Not Correct Material Weaknesses
Project No. D2010-D000FI-0234.000

Recommendation.

A.1. We recommend that the Director, Army Office of Business Transformation and Assistant Secretary of the Army (Financial Management and Comptroller) develop a plan of action and milestones to bring the Logistics Modernization Program system into compliance with the DoD Business Enterprise Architecture Procure-to-Pay business rules. Specifically, as part of the Army Business System Information Technology Strategy, define the Army's plans for developing effective and efficient Logistics Modernization Program system business processes that will:

a. Integrate the contracting and entitlement functions.

b. Expedite a solution for resolving the in-transit inventory posting logic problems and correct abnormal balances.

c. Reassess the system's accounts payable business process flow and posting logic and determine whether additional problems exist that cause abnormal balances. If so, develop the corrective actions needed to resolve those problems.

d. Develop performance indicators to assist in identifying the potential for significant posting errors and develop responsive corrective actions.

e. Develop the edit checks and business workflows needed to control and route purchase requests and Military Interdepartmental Purchase Requests to the appropriate individuals for approval and funds certification. This should include:

(1) Associating fund codes and approval authority to an individual's assigned activity.

(2) Assigning certification of funds availability to a limited number of individuals and developing the requirement for the system to limit funds certification to only these individuals.

(3) Directing that fund managers establish commitments for purchase requests at the time an activity releases the requests for obligation actions.

(4) Developing the functionality needed for separate individuals to create and accept Military Interdepartmental Purchase Requests within the system.

(5) Validating the data contained in the Program Activity Table and ensuring that it is preparing manual documents correctly and developing compensating controls to validate the data integrity of manually created obligations.

f. Identify offline systems and procedures within the Procure-to-Pay phases, incorporate the functionality into the system, and discontinue the use of offline processes. In situations where Army managers cannot immediately incorporate the functionality, develop compensating controls over non-integrated offline processes and restrict the creation of manual commitment and obligation transactions to resource management personnel.

g. Develop functionality within the system to capture and record the actual vendor invoice date, vendor invoice number, and date of invoice receipt at the paying station. Also, develop the data fields needed to record separately the actual receipt and acceptance dates for goods and services.

h. Develop the ability to identify all documents related to Procure-to-Pay transactions within a single system query.

i. Develop a ready-to-pay file based on the system's approval of prevalidation requests.

Army Response: **Concur.** We recognize that there are opportunities to improve the efficiency of procure to pay (P2P) processing in the Logistics Modernization Program (LMP). Current process segmentation adds to interface complexity and error rates and is a source of abnormal balances. Our current system design, however, is normal for typical ERP implementation best practice. Best practice is to reduce risk associated with "grand design" implementation projects by first fielding a basic capability and then capitalizing on investment via driving more functionality into the system. As part of the Army Business System Information Technology Strategy (BSIT), we will review the feasibility of integrating additional P2P functionality within the LMP environment to include recommendations in this audit report. Results of the review will be used to develop a plan of action and milestones (POAM) addressing the viability of integrating additional contracting and entitling functions, improving internal controls, identifying and correcting abnormal balances relating to P2P transactions, and developing and tracking additional metrics and performance indicators. Our POAM will reflect limitations imposed by the Department's Business Enterprise Architecture related to contract writing, vendor invoicing, payment entitlements and disbursement processing.

Although the feasibility analysis and P2P POAM will identify additional opportunities to enhance LMP P2P processing, significant improvements were made during 2011. For example, we corrected the current configuration for contract authority, corrected posting logic for IMPAC expenses, enhanced configuration of Defense Travel System (DTS) and Integrated Product-Support Vendor (IPV) transactions. Additionally, our December 2011 software release added capabilities for constructive receipts, automated in-transit inventory accrual processes, improved the derivation of Federal vs. Non-Federal indicator, corrected posting logic resulting in the reduction of abnormal balances, and improved access controls to prevent inaccurate cross-command postings. These improvements enabled a $1.9 billion reduction in abnormal balances between August and December 2011.

The Army will continue to leverage the Business System Information Technology (BSIT) strategy and governance procedures to implement additional improvements as updates to the Standard Financial Information Structure (SFIS) and Business Enterprise Architecture (BEA) are published. We are currently in requirements definition discussions for Local Vendor Pay (LVP) enhancements enabling LMP to perform vendor payment entitlement functions currently handled by the Computerized Accounts Payable System – Windows (CAPS-W). These requirements include edit checks and business workflows needed to control and route purchase requests and Military Interdepartmental Purchase Requests (MIPRs) through LMP to the appropriate individuals for approval and funds certification, management of vendor data, and entitlement functions. We expect to complete our requirements analysis by March 2012.

A.2. We recommend that the Assistant Secretary of the Army (Financial Management and Comptroller) direct the Army Materiel Command G-8 to:

a. Conduct a review of the unobligated authority general ledger account balances to determine whether an Antideficiency Act violation occurred, and take actions to correct the abnormal balances and posting logic problems related to the accounts.

b. Modify the Logistics Modernization Program system to cease the automatic obligation of unmatched disbursements until activities accomplish proper reconciliation as required by the DoD Financial Management Regulation.

c. Develop a system edit check that identifies when an activity exceeds the allotment contained in General Ledger Account Code 4610 and require activities to report each occurrence to the Office of Assistant Secretary of the Army (Financial Management and Comptroller) for immediate resolution.

Army Response: **Concur.** We will direct HQAMC to work with Defense Finance and Accounting Service (DFAS) Columbus to review all limits and determine if any are over-obligated. If this review discloses an Antideficiency Act violation has occurred, appropriate action will be taken. Abnormal balances disclosed by the review will be corrected. We will complete this review by June 2012. Army is in the process of determining a compliant process so that it can discontinue the automatic obligation process for UMDs (ZK process). We will conduct a workshop in March 2012 with HQAMC, LMP PM, DoDIG, and DFAS to determine a compliant process and provide milestones for transitioning to that process. Recognizing that there are some limitations on customizing SAP, we will make use of existing reports to better monitor and flag potential issues with GLAC 4610. We will include milestones related to those actions in the P2P POAM developed in response to Recommendation A.1.

A.3. We recommend that the Assistant Secretary of the Army (Financial Management and Comptroller) direct the development of a comprehensive internal control program for the Logistics Modernization Program Procure-to-Pay business process to assess the quality of performance and regular management and supervisory activities over the business process. Army managers should work with Logistics Modernization Program Project Office personnel to ensure that they design and implement the necessary procedures and controls and develop the testing needed to ensure control effectiveness.

Army Response: **Concur.** As part of our Financial Improvement Plan audit readiness discovery and evaluation activities, we will assess key controls supporting all Financial Improvement and Audit Readiness (FIAR) assessable units, including those related to procure to pay activities. The assessment will determine the effectiveness of the design and operation of applicable controls and identify corrective actions required to bring controls into compliance with audit standards. The assessment might also recommend establishing a standard performance objective for those managers and supervisors working P2P processes. These actions will be completed during FY 2013.

B.1. We recommend that the Assistant Secretary of the Army (Financial Management and Comptroller) develop a plan for the Army Materiel Command to improve system access controls within the Logistics Modernization Program system. Specifically:

a. Determine the impact of regulatory requirements, such as the Certifying Officer's Legislation, on the development and issuance of the functional security role templates. Within 60 days of the report, identify and correct missing and deficient official appointment documentation before allowing access to the templates. Once identified, supervisors and system administrators should ensure the proper appointment of users before granting access to the templates containing those functions.
b. Perform a risk assessment of the Logistics Modernization Program system transaction screens assigned within each of the functional security role templates and minimize the potential for segregation of duties conflicts. Once this assessment is completed, managers should redesign the templates to cover the specific job functions performed at

each activity and limit user access to only those transaction screens needed to perform those job functions.

c. Require the mapping of each functional security role template to the Procure-to-Pay business process to determine the existence of potential segregation of duty and least privilege conflicts. If conflicts exist, realign the transaction screens as necessary to prevent these conflicts.

d. Update the Logistics Modernization Program User Access Policy and include detailed procedures that prescribe:

(1) How administrators and supervisors should assign functional security roles to users.

(2) How to manage user access to include the use of approval databases or another tracking mechanism.

(3) How administrators should perform regular review of system access accounts suspended due to inactivity and work with supervisors to suspend or remove all roles when a user departs a work unit, leaves an activity installation, or loses a security clearance and obtain approval by the new supervisor of all access granted after reassignment.

e. Conduct an initial review of system access, at all levels, to identify users who have been granted unneeded access and, thereafter, conduct periodic reviews of system access.

f. Develop a method to monitor the assignment of functional security roles at the highest level and ensure that activities conduct the required periodic reviews.

Army Response: Concur. ASA(FM&C) will direct HQAMC and DFAS to perform a comprehensive review of LMP system controls. The review will cover access controls, interface controls, process controls, configuration controls, and data integrity. It will identify system access deficiencies and risk; and provide an approach for improving them. Necessary risk assessments, compensating control review, role mapping, acquisition of provisioning tools/systems to identify and mitigate SOD issues, and policy updates will be included as part of the effort. The review will begin on/about March 2012.

Army and HQAMC will provide business rules for handling Segregation of Duty (SOD) conflicts to update Functional Security Roles (FSRs). Many of the FSRs across the enterprise are already standard. Until Governance, Risk and Compliance (GRC) implementation we will continue to use existing meetings and policy to minimize Segregation of Duties conflicts. The HQAMC User Account Manager Policy was signed by HQAMC, Chief Information Officer, on January 24, 2012. Managers and supervisors receive training on the use of the User Account Management system on a regular and ad hoc basis as system and personnel changes occur. The policy stipulates the review of all suspended inactive accounts on an annual basis to determine if access is still required. Army is in the process of reviewing appointment documentation. Additional requirements will be identified in the POAM developed in response to Recommendation A.1.

B.2. We recommend that the Assistant Secretary of the Army (Financial Management and Comptroller) work with the Army Materiel Command to:

a. Provide centralized training for administrators and supervisors on how to use functional security role templates to administer access and prevent conflicts.

b. Purchase the system software needed to assist in developing the system controls needed to prevent or identify excessive or unauthorized access, or identify and develop compatible system controls using other means.
c. Control administrator roles and prevent administrators from assigning functional security roles to themselves or develop appropriate compensating controls.

Army Response: **Concur.** Upon completion of the review in Recommendation B.1, the Army will be in a better position to identify training requirements, target audiences, and the right automated tool to handle provisioning of users and controlling system roles/permissions. Within 60 days of the review, Army and HQAMC will review current training requirements and adjust accordingly. The new HQAMC User Account Manager Policy addresses functional security role assignments and the mitigation of segregation of duties conflicts. HQAMC G-6 will conduct periodic reviews to ensure UAMs are not assigning themselves privileges and will take action for any user violating their privileges. HQAMC G-6 will oversee and instruct the commands on how to conduct an annual UAM review during 3rd quarter of FY2012. Additional corrective requirements will be addressed in the POAM developed in A1.

LMP went live without Governance, Risk and Compliance (GRC) SAP functionality. However, there are plans to begin configuration of the GRC functionality in February 2012 with an implementation date of December 2012. GRC is an automated risk and compliance monitoring activity which will proactively mitigate risk and provide system controls needed to prevent or identify excessive or unauthorized access and segregation of duties conflicts. FSRs will be reviewed and if necessary redesigned after GRC implementation to minimize risk.

C.2. We recommend that the Director, Army Office of Business Transformation and Assistant Secretary of the Army (Financial Management and Comptroller) direct in policy that the:

a. Army Enterprise Systems Integration Program Manager serve as the vendor master data manager with the authority and personnel to:

(1) Require all systems doing business with the Army to use only the vendor master to populate business partner information.
(2) Prevent Army Enterprise Resource Planning system users from creating, modifying, or deleting vendor information and only allow for view access to master data by other system users.
(3) Validate the integrity of the business partner information contained in the vendor master records.
(4) Create all business partner records from information contained in the Federal Agency Registration and Central Contractor Registration.
(5) Establish individual business partner records using the Business Partner Network number and create data files to populate the applicable Standard Financial Information Structure attributes.
(6) Issue instructions on the administration and use of Army vendor information.

b. Routing Identifier Code locations register within Federal Agency Registration database before creating a business partner record in the Army vendor master record for doing business transactions with the Army or accepting any supplemental business partner information from that location.

c. Army Enterprise Resource Planning Project Offices:

(1) remove functional security roles capable of adding, revising, or deleting vender information; and

(2) cease developing change requests for correcting of vendor master data.

Army Response: Concur. The Army's business strategy is managed by the Office of Business Transformation. The "Army Business Systems Information Technology Strategy" dated February 14, 2011 serves as the Army's foundation and roadmap for executing our enterprise architecture. The BSIT states that AESIP synchronizes and syndicates select enterprise master data applicable to each Army ERP system. Additionally, AESIP supports integration hub services for each system, as applicable. The BSIT strategy is a living document and will evolve in response to changes. Consequently, AMC and ASA (FMC) personnel will work with OBT personnel to reevaluate and adjust as necessary the functions of the AESIP PM and his role as the vendor master data manager. The Army will continue to leverage the Business System Information Technology (BSIT) strategy and governance procedures to implement additional improvements as updates and opportunities avail themselves.

C.3. We recommend that the Army Enterprise Systems Integration Program Manager create and manage a vendor master based on the System for Award Management database that can:

a. Populate required vendor-related Standard Financial Information Structure attributes with valid domain values.

b. Establish the Business Partner Network number as the key data field for all business partner records and use that data field when receiving and sending information to Army and other systems.

c. Identify and track the business partner registration status in the Central Contractor Registration and Federal Agency Registration databases and System for Award Management database once implemented.

d. Obtain all vendor information needed by Army Enterprise Resource Planning systems and supporting systems.

Army Response: Concur. The PM AESIP will work with the stakeholders to implement this recommendation. Actions taken will require policy, system and process changes, and validation of Army vendor data to ensure that it is in sync with SAM vendor data.

With respect to SAM, according to the latest data element listing at General Services Administration, the BPN term will not be used. Commercial and non-government entities will register with their DUNS number and it will be stored in the SAM DUNS # field. DoD agencies will register with their DODAAC and it will be stored in the SAM DODAAC field. The AESIP vendor master will be enhanced to be in line with the new data. We will work with LMP on the best and most cost effective approach to have their system support the design. Ideally, performing all fed/non-fed derivations in AESIP, syndicating the results to the other systems, and prohibiting changes anywhere except in AESIP is the desired goal. A cost-benefit analysis will be required to determine if this yields a tangible return on investment.

Actions related to item C.3.c. are completed. AESIP currently receives the registration status and passes this information to the ERPs and will continue to receive and provide this information with the migration to SAM.

C.4. We recommend that the Assistant Secretary of the Army (Financial Management and Comptroller) validate that the Logistics Modernization Program system has controls in place to reject new contracts and payment requests from business partners with inactive vendor registration flags.

Army Response: **Concur.** Army will validate transactional data as part of internal control assessment. The test will include a validation of business partner data in LMP compared to the data for that business partner in AESIP. This validation will occur after we have implemented SAM, but not later than September 30, 2012. Additional requirements will be addressed in the POAM developed in response to Recommendation A.1.

Inspector General
Department of Defense