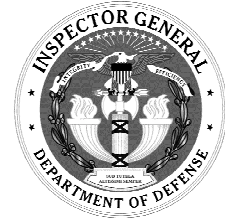

October 3, 2002



Information Technology

Information Resource Management
at the Army Aviation and Missile
Command
(D-2003-002)

Department of Defense
Office of the Inspector General

Quality

Integrity

Accountability

Report Documentation Page

Report Date 03 Oct 2002	Report Type N/A	Dates Covered (from... to) -
Title and Subtitle Information Technology: Information Resource Management at the Army Aviation and Missile Command	Contract Number	
	Grant Number	
	Program Element Number	
Author(s)	Project Number	
	Task Number	
	Work Unit Number	
Performing Organization Name(s) and Address(es) OAIG-AUD (ATTN: AFTS Audit Suggestions) Inspector General, Department of Defense 400 Army Navy Drive (Room 801) Arlington, VA 22202-2884	Performing Organization Report Number D-2003-002	
	Sponsoring/Monitoring Agency Name(s) and Address(es)	
		Sponsor/Monitor's Acronym(s)
		Sponsor/Monitor's Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited		
Supplementary Notes		
Abstract		
Subject Terms		
Report Classification unclassified	Classification of this page unclassified	
Classification of Abstract unclassified	Limitation of Abstract UU	
Number of Pages 35		

Additional Information and Copies

To obtain additional copies of this report, visit the Web site of the Inspector General of the Department of Defense at www.dodig.osd.mil/audit/reports or contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Audits

To suggest ideas for or to request audits, contact the Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General of the Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, DC 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

AMCOM
CIO

Army Aviation and Missile Command
Chief Information Officer



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

October 3, 2002

MEMORANDUM FOR AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: Report on Information Resource Management at the Army Aviation and
Missile Command (Report No. D-2003-002)

We are providing this report for your review and comment. We considered management comments on a draft of this report when preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. We request that the Army provide additional comments on Recommendations 2, 4, 5, and 6 and provide a completion date for Recommendation 3 by December 3, 2002.

If possible, please provide management comments in electronic format (Adobe Acrobat file only). Send electronic transmission to the e-mail address cited in the last paragraph of this memorandum. Copies of the management comments must contain the actual signature of the authorizing official. We cannot accept the /Signed/ symbol in place of the signature. If you arrange to send classified comments electronically, they must be sent over the classified SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the audit staff. Questions on this audit should be directed to Mr. Charles M. Santoni at (703) 604-9051 (DSN 664-9051) (csantoni@dodig.osd.mil) or Mr. David M. Wyte at (703) 604-9027 (DSN 664-9027) (dwyte@dodig.osd.mil). See Appendix E for the report distribution. The team members are listed inside the back cover.

A handwritten signature in cursive script that reads "David K. Steensma".

David K. Steensma
Deputy Assistant Inspector General
for Auditing

Office of the Inspector General of the Department of Defense

Report No. D-2003-002

October 3, 2002

(Project No. D2001AL-0173)

Information Resource Management at the Army Aviation and Missile Command

Executive Summary

Who Should Read This Report and Why? Chief Information Officers and others who manage information technology resources within DoD should read this report because the issues identified may be applicable across DoD.

Background. This audit was initiated in response to a Hotline allegation that the Army Aviation and Missile Command (the Command) was not properly managing information resources at the Redstone Arsenal, Huntsville, Alabama. The Command develops, acquires, fields, and sustains aviation and missile systems for Army battlefield systems and provides support services to more than 40 tenants co-located at the Redstone Arsenal and the surrounding area. For FY 2001, the Command budget at the Redstone Arsenal exceeded \$7.1 billion, and identified costs for information technology were estimated to be as much as \$126 million.

Results. The Command was not effectively managing information resources at the Redstone Arsenal. Although the Chief Information Officer was engaged in the Command's investment and architecture strategy, information technology purchases of more than \$1.5 million were not coordinated and deliverables did not meet software and accreditation standards. The Command must allow the Chief Information Officer to become more involved in the business decision processes of its organizations when they acquire information technology. In addition, untrained personnel made quality acceptance recommendations for more than \$11.5 million in purchases; purchase card holders made more than \$1 million in unapproved acquisitions; and the Command did not realize a potential \$431,000 annual cost avoidance by combining modules of similar systems. Management controls need to be put in place to ensure that personnel who make quality acceptance recommendations for purchases receive training in basic information technology concepts and to ensure that only approved cardholders acquire information technology products and services. Further, the Command needs to reassess the feasibility and cost effectiveness of combining similar system modules.

The Command's management control evaluation for information management did not include all resources at the Redstone Arsenal. Further, when a Chief Information Officer-sponsored information technology study reported that the Command was not following best practices, the Command chose not to report the material weaknesses or the actions that it was taking to correct the weaknesses in its FY 2001 Annual Statement of Assurance. The Command needs to evaluate all information management and information technology functions of Redstone Arsenal and report actions to correct any material weaknesses in its FY 2002 Statement of Assurance. For details of the audit results and recommendations, see the Finding section of the report. For a discussion of the allegation, see Appendix C.

Management Comments and Audit Response. The Chief of Staff, Army Materiel Command, responding for the Commanding General, Army Aviation and Missile Command, generally concurred with the recommendations. The Command will develop a curriculum and provide training for evaluating the quality of information technology purchases within 3 to 6 months. Also, the Command will develop an automated system for managing information technology requirements and purchase card transactions. Further, the Command believes that existing controls and the comprehensive Information Management Master Plan that it developed in April 2002 will increase the Chief Information Officer's involvement in information technology initiatives. However, the Command stated that combining modules of similar systems was not feasible or cost-effective. In addition, the Command stated that it only reports management control weaknesses that it cannot readily correct in its statements of assurance. Accordingly, after re-evaluating recommendations made in the FY 2001 information technology study, the Command will report weaknesses that cannot be corrected. See the Finding section of the report for a discussion of management comments and the Management Comments section for the complete text of the comments.

The comments did not fully meet the intent of the recommendations. Existing controls and the April 2002 Information Management Master Plan will not ensure that the Chief Information Officer is involved in all information technology initiatives. The Master Plan is a strategy only, and additional control guidance will be required to establish procedures for reviews and evaluations by the Chief Information Officer. Also, the Command's decision and justifications for not combining modules of similar systems were not documented and communicated to the involved Command organizations. After the decision was made, an involved organization believed that the combination was feasible. Further, the Command's practice of selectively reporting management control weaknesses in statements of assurance does not comply with Army guidance. Information technology is a DoD high-risk area. Therefore, the FY 2001 information technology study results should have been elevated to the Army Materiel Command. Additionally, the Command did not provide an implementation date for its planned requirements and purchase card transaction management system for information technology. We request that the Army reconsider its position on the recommendations and provide additional comments by December 3, 2002.

Table of Contents

Executive Summary	i
Background	1
Objectives	1
Finding	
Managing Army Aviation and Missile Command Information Resources	2
Appendixes	
A. Scope and Methodology	11
Management Control Program Review	13
Prior Coverage	13
B. Mandatory Guidance	14
C. Validation of Assertions Made in the Hotline Allegation	17
D. Information Resource Management at Redstone Arsenal	19
E. Report Distribution	21
Management Comments	
Department of the Army	23

Background

We performed this audit in response to a Defense Hotline referral. The anonymous source alleged that the Army Aviation and Missile Command (AMCOM), located at the Redstone Arsenal, Huntsville, Alabama, was not properly managing information resources. The report discusses the quality of AMCOM information management and addresses the validity of the claims raised by the anonymous source. See Appendix C for details on the validation of assertions made in the Hotline Allegation.

AMCOM develops, acquires, fields, and sustains aviation and missile systems to guarantee the readiness and technological superiority of Army battlefield systems. AMCOM Directorates and Centers implement that mission and provide support services to more than 40 tenants co-located at the Redstone Arsenal and the surrounding area. For FY 2001, the AMCOM budget at the Redstone Arsenal exceeded \$7.1 billion. The AMCOM Corporate Information Center, under the direction of the Chief Information Officer (CIO), designs, develops, implements, and maintains all aspects of information management and technology at the Redstone Arsenal. For FY 2001, identified AMCOM costs for information technology were estimated to be as much as \$126 million.

Objectives

The audit evaluated the management of information resources at AMCOM. Specifically, the audit determined whether AMCOM was managing information resources in accordance with Office of Management and Budget and DoD guidance. Further, the audit was to determine whether AMCOM had reengineered its business processes in response to planned system deployments of the Army's Wholesale Logistics Modernization Plan.¹ However, after we announced our objective, we determined that AMCOM had not reengineered its business processes because applications for the Army Wholesale Logistics Modernization Plan had not been completed. Also, we reviewed the management control program related to the objectives. See Appendix A for a discussion of the audit scope and methodology and the review of the management control program.

¹The Wholesale Logistics Modernization Plan is a 10-year, \$680 million initiative that replaces the Army's Command Commodity Standard System and Standard Depot System with commercial-off-the-shelf applications that are operated and maintained by the Computer Sciences Corporation.

Managing Army Aviation and Missile Command Information Resources

The AMCOM Chief Information Officer (CIO) was not effectively managing information resources because the Commanding General's organizational elements and tenants at the Redstone Arsenal acquired information technology without engaging the CIO and the Corporate Information Center in their information management decisions. As a result, the Command allowed:

- personnel who had no information technology training to make quality review recommendations for the acceptance of more than \$11.5 million in information technology deliverables during FY 2001;
- organizational elements and tenants to purchase more than \$1.5 million for information technology products and services in FY 2001 without being reviewed by the Corporate Information Center;
- unapproved purchase card holders to obtain more than \$1 million in information technology products during FY 2001;
- an uncertified and unaccredited hardware installation that resulted in a security breach;
- the purchase of a training module that did not comply with software standards for people with disabilities; and
- a potential annual cost avoidance opportunity, estimated to be as much as \$431,000, to be missed by not combining the Automated Resource Management System and the Integrated Center Information System.

Also, the AMCOM management control evaluation for information management did not include all resources managed and funded by organizational elements and tenants at the Redstone Arsenal. Further, when a CIO-sponsored information technology study reported that AMCOM was not following best practices for the information management and information technology functions, AMCOM chose not to report the material weaknesses cited in the study or the actions that it was taking to correct the weaknesses to the Army Materiel Command in its FY 2001 Annual Statement of Assurance.

Mandatory Guidance

Office of Management and Budget and DoD guidance implement the Clinger-Cohen Act of 1996 by providing managers with policies and procedures for managing and safeguarding information resources and for evaluating

management controls. Further, Army and AMCOM regulations state that information must be managed as any other asset, with CIO involvement in decisions affecting information technology equipment, systems, software, services, or alternative solutions. Also, the General Accounting Office has identified the management of information technology investments as a high-risk area for the DoD. Appendix B describes the guidance relating to the management of information resources at the Redstone Arsenal.

Monitoring Information Management

At AMCOM, the span of management control for the CIO does not extend beyond the Corporate Information Center. As a result, AMCOM organizations and tenants manage and fund mission-related information resources without engaging the CIO and the Corporate Information Center in their information technology decisions. Therefore, the CIO did not directly manage and control a significant portion of information technology funds. We estimated² that about \$44 million, or 35 percent, of the FY 2001 funds for information technology was not controlled by the CIO. Further, except for the Corporate Information Center, expenditures for information technology were included with expenditures for other mission activities and therefore were not fully identifiable. Appendix D demonstrates the extent of information technology resources maintained and controlled by AMCOM organizational elements and major tenant organizations.

Benchmark Study

A benchmark study³ sponsored by the CIO concluded that AMCOM information resources were not being efficiently and effectively managed due to limited support from the Command's senior management. The \$99,916 study, conducted between June 2000 and March 2001, found the following conditions at AMCOM.

- Multiple formal and informal information technology organizations existed that operated outside the purview of the CIO-managed Corporate Information Center.
- Independent network and computer ownership resulted in chaotic and inefficient support.
- Systems were implemented without Corporate Information Center input and, when migrated to the Center, would require support from untrained personnel.

²Estimate is based on discussions with personnel responsible for information resource management at AMCOM and tenant organizations and reviews of information technology contracts.

³“U.S. Army Aviation and Missile Command Distributed Computing Environment (DCE) Benchmark Study,” March 28, 2001, prepared for AMCOM by the Harris Corporation.

-
- Existing infrastructure support was inadequate with little hope of scaling up to meet future needs.
 - The Corporate Information Center was unable to meet current demands due to resources being extended for other priorities.
 - The Corporate Information Center was attempting to manage multiple generations of assets with limited staff and training.
 - Help Desk assistance was inadequate for customer information technology support.
 - Asset management did not allow efficient tracking and use of resources.

In response to the study, AMCOM formed integrated process teams, chaired by the CIO, to systematically analyze and find solutions to the identified issues. The Business Information Management Planning Board drafted an Information Management Master Plan, and the Information Technology Team developed guidance for information technology best business practices and processes.

Information Management Master Plan. The AMCOM Information Management Master Plan provides the Command with guidance for implementing information management goals and objectives. The document was a collaborative effort of all the AMCOM major organizational elements and placed the CIO at the top of the AMCOM information management chain.

Best Business Practices. The Information Technology Team identified five business cases or areas of improvement. The most significant case addresses architecture for hardware and software, and processes that should be changed to achieve the standardization objective. The team planned to complete policies and procedures for implementation by July 2002. Further, the team will continually meet to discuss the identified business areas.

Although AMCOM took actions as a result of the benchmark study, organizational elements and tenants at the Redstone Arsenal did not always engage the CIO and the Corporate Information Center in information management decisions.

Information Technology Acquisitions

Our analysis of the assertions made in the Defense Hotline allegation (see Appendix C) showed that the Commanding General and the CIO had limited oversight of information products and services received by AMCOM organizational elements and tenants. As a result, personnel untrained in information technology made quality acceptance recommendations for deliverables received from the Information Mission Area Support Services Contract; organizations did not coordinate information technology requirements with the Corporate Information Center as required; purchase card holders made

unauthorized information technology acquisitions; deliverables did not conform to information technology and security standards; and AMCOM did not realize a potential recurring cost avoidance.

Information Mission Area Support Services Contract. Technical acceptances of services obtained from the Information Mission Area Support Services Contract⁴ relied on evaluations made by technical monitors; however, not all monitors were trained in information technology. We determined that AMCOM did not provide 31 of the 48 assigned technical monitors with information technology training or guidance for evaluating the quality of deliverable services. As a result, in FY 2001, more than half the funds obligated for information support services were recommended for acceptance by personnel who had no formal training in information technology. Cumulatively, these contracted deliverables amounted to more than \$11.5 million of the \$23 million invested for information mission area support services.

Coordination of Requirements. Contrary to AMCOM Regulation 25-4, "Information Management," June 9, 1999, requirements for information services and products were not always coordinated with the CIO and the Corporate Information Center. AMCOM Regulation 25-4 requires CIO approval before organizational elements purchase information technology for business systems. Without that coordination, the CIO and the Corporate Information Center were unaware of the extent and the quality of information technology acquired by AMCOM organizational elements and tenants.

Aviation and Missile Research, Development and Engineering Center Contract. Information technology services obtained through the Aviation and Missile Research, Development, and Engineering Center Contract⁵ were not always reviewed by the CIO and the Corporate Information Center. Of eight orders for information technology services issued between March 2001 and November 2001, only one, valued at \$19,995, was coordinated through the Corporate Information Center. Cumulatively, the seven orders that were not coordinated totaled more than \$1.5 million. According to responsible personnel, coordination was not required for the information technology requirements within the Aviation and Missile Research, Development, and Engineering Center.

Purchase Card Acquisitions. Personnel with purchase card privileges obtained information technology products without prior approvals from the Deputy CIO. AMCOM Regulation 25-4 requires that cardholders receive annual authorizations to purchase information technology products. A comparison of FY 2001 information technology transactions to approvals showed that eight cardholders had purchased information technology products

⁴A 5-year, cost-plus-fixed-fee contract awarded to Nichols Colsat Information Management of Huntsville, Alabama, for automation, telecommunications, visual information, and records management services.

⁵A cost-reimbursable, \$12.3 million no-fee contract awarded in March 2001 to the University of Alabama in Huntsville for system engineering and advanced weapon system and manufacturing technology support used by the Research, Development, and Engineering Center.

without obtaining prior authorizations. Our analysis of the transactions made by seven of those cardholders, showed that:

- two cardholders had expired authorizations,
- two cardholders believed that authorizations to purchase information technology products extended to them when another person in their office had received approval, and
- three cardholders were unaware of the AMCOM requirement to obtain an approval to purchase information technology products.

Cumulatively, the eight cardholders made 332 transactions and acquired information technology software, hardware, and services worth more than \$1 million in FY 2001. One cardholder made 177 purchases totaling more than \$589,000. We concluded that those purchases went undetected because AMCOM had not implemented a management control procedure to screen purchase card transactions for information technology software, hardware, and services. Our analysis of credit card transactions was limited to identifying those personnel who were using credit cards to purchase information technology products and determining whether those personnel had obtained authorizations to purchase information technology. We did not perform tests to determine whether the credit card purchases were justified.

Army Regulation 380-19, "Information Systems Security," February 27, 1998, requires that automated information systems be certified and accredited for information assurance before being deployed. Unaware of the requirement, the Command Analysis Directorate used a purchase card to obtain a graphics writer for \$14,013 and connected it to the Redstone Arsenal campus area network. In October 2001, an Army computer emergency response team outside the Command found that the installed writer allowed an undetected intrusion to its stored files. According to AMCOM security personnel, violations of the campus area network may have occurred. Without a process for monitoring purchase card transactions, security personnel were unaware of the presence of the graphics writer until notified of the breach.

Training Module. The Intelligence and Security Directorate acquired a security awareness training module for \$59,659 without allowing the Corporate Information Center an opportunity to evaluate the contract. When the Corporate Information Center reviewed the deliverable for compatibility with the campus area network, the module had to be modified because it did not comply with Federal standards for people with disabilities. According to Office of Management and Budget Circular A-130, "Management of Federal Information Resources," November 30, 2000, agencies must ensure that persons with disabilities have reasonable access to information products.

Resource Management Systems. Similar information systems for managing resources were operated, maintained, and continually upgraded at AMCOM. In September 1998, a joint cost analysis team from the Research Development and Engineering Center and the Corporate Information Center concluded that AMCOM would avoid as much as \$431,000 annually by combining modules

from their resource management systems. However, the Deputy Director of the Research Development and Engineering Center recommended delaying action pending further study. As of November 2001, the modules had not been combined. Further, AMCOM officials could not find documentation to show that additional study had resumed in response to the recommendation.

Management Control Evaluations and Reports

Management control reviews and reports did not demonstrate that AMCOM had effectively managed risks for the information management function. Army Regulation 11-2, "Management Control," August 1, 1994, requires commanders and managers to establish and maintain effective management controls, assess areas of risk, identify and correct weaknesses, and report weaknesses to the next higher level of command. In addition, Regulation 11-2 requires managers to give high priority to weaknesses in identified high-risk areas. Also, Army Regulation 25-1, "Army Information Management," February 15, 2000, provides a checklist to evaluate management controls for information management and information technology functions.

The General Accounting Office has identified the management of information technology investments as a high-risk area for the DoD. AMCOM evaluated information system security in FY 1999 and found that insufficient funding delayed program implementation. In its FY 2000 and FY 2001 Statements of Assurance, AMCOM reported the delayed implementation as an uncorrected material weakness. However, when AMCOM evaluated management controls for information management and information technology in FY 2000, it limited its review to the Corporate Information Center, excluding information resources that were functionally managed and funded by other organizational elements and tenants. Further, when the CIO-sponsored benchmark study of information management found that AMCOM was not following information technology best practices, AMCOM chose not to report the material weaknesses cited in the study or the actions it was taking to correct these weaknesses to the Army Materiel Command in its FY 2001 Annual Statement of Assurance.

Summary

At AMCOM, the mission function of collecting, storing, and reporting information extends beyond the Corporate Information Center. Although the CIO initiated actions to develop and implement a Command strategy for information management investments and architecture for hardware and software, the CIO and the Corporate Information Center were not always engaged in decisions affecting the acquisition and operation of information resources. Accordingly, the CIO and the Corporate Information Center must become involved in the business decision processes of AMCOM and tenant organizations to effectively manage and oversee their information technology resources.

Management Comments on the Finding

The Chief of Staff, Army Materiel Command stated that he considered the report's finding and recommendations to be generally true throughout DoD and across many government agencies. Further, he believed that the new Army Knowledge Management directives will resolve reported issues.

Recommendations, Management Comments, and Audit Response

We recommend that the Commanding General, Army Aviation and Missile Command:

1. Provide technical monitors with training and guidance in the basic information technology concepts necessary to evaluate the acceptability of products and services obtained from the Information Mission Area Support Services Contract.

Management Comments. The Chief of Staff, Army Materiel Command, responding for the Commanding General, Army Aviation and Missile Command, generally concurred with the recommendation. The Army Aviation and Missile Command plans to develop a curriculum and provide training for evaluating the quality of information technology services. The Command anticipates implementing the training within 3 to 6 months.

2. Establish controls to ensure that the Army Aviation and Missile Command and tenant organizations engage the Chief Information Officer in business system acquisitions of information technology in accordance with Army Aviation and Missile Command Regulation 25-4, "Information Management."

Management Comments. The Chief of Staff, Army Materiel Command concurred with the intent of the recommendation. The Chief of Staff stated that the Army Aviation and Missile Command developed a comprehensive Information Management Master Plan in April 2002 to strengthen controls. The plan, in conjunction with existing procedures, will enable the Chief Information Officer to become more involved in reviews and evaluations of information technology initiatives.

Audit Response. The comments are partially responsive. The Army Aviation and Missile Command continues to assume that the Chief Information Officer will review and evaluate all information technology initiatives as a result of its existing controls and the April 2002 Information Management Master Plan. The audit demonstrated that multiple information technology organizations exist outside the direct control of the Chief Information Officer. Further, the Information Management Master Plan is a strategy and not a business process procedure. Without additional control guidance, we believe that Command organizations will not always engage the Chief Information Officer in business

decisions affecting information technology. Therefore, we request that the Army reconsider its position on this recommendation and provide additional comments in response to the final report.

3. Screen purchase card transactions to ensure that information technology products and services are acquired by approved cardholders.

Management Comments. The Chief of Staff, Army Materiel Command concurred and stated that the Army Aviation and Missile Command is developing an automated system that will manage information technology requirements and purchase card transactions.

Audit Response. The planned action satisfies the intent of the recommendation. However, the Army needs to provide a system completion date in response to the final report.

4. Reassess the identified annual cost avoidance opportunity of combining the Automated Resource Management System and Integrated Center Information System modules.

Management Comments. The Chief of Staff, Army Materiel Command nonconcurred and stated that in September 1998 the Army Aviation and Missile Command determined that the combination of system modules was not feasible or cost-effective.

Audit Response. The Army Aviation and Missile Command could not provide documentation supporting its decision not to combine the system modules. Further, subsequent correspondence within the Command, dated January 8, 1999, stated that the combination was feasible and that a final decision had not been made. Therefore, we request that the Army reconsider its position on this recommendation and provide additional comments in response to the final report.

5. Report the actions taken to correct weaknesses in information management and information technology best practices contained in the “U.S. Army Aviation and Missile Command Distributed Computing Environment (DCE) Benchmark Study” in the Aviation and Missile Command FY 2002 Statement of Assurance and subsequent statements until actions are completed.

Management Comments. The Chief of Staff, Army Materiel Command concurred with the intent of the recommendation and stated that the Army Aviation and Missile Command is reevaluating the recommendations made in the Benchmark Study and that material weaknesses, which cannot be readily corrected, will be reported through proper channels.

Audit Response. The comments are partially responsive. Because information technology is recognized as a DoD high-risk area, the Army Aviation and Missile Command should report the Benchmark Study results and the subsequent actions taken to improve information technology business practices

to the Army Materiel Command in its statements of assurance. Therefore, we request that the Army provide additional comments in response to the final report.

6. Evaluate all Redstone Arsenal information management and information technology functions and report any material weakness in the Army Aviation and Missile Command FY 2002 Statement of Assurance.

Management Comments. The Chief of Staff, Army Materiel Command concurred with the intent of the recommendation. He stated that the Chief Information Officer at the Army Aviation and Missile Command has implemented and improved many information management business processes to allow better management controls and accountability of information technology resources. In addition, the Army Aviation and Missile Command will continue to review existing information technology processes and report material weaknesses that it cannot correct.

Audit Response. The Army Aviation and Missile Command's practice of selectively reporting only weaknesses that it cannot correct in statements of assurance is contrary to Army guidance. Army management control guidance requires commanders and managers to keep superiors informed and to identify and correct weaknesses in known high-risk areas. Therefore, we request that the Army reconsider its position on this recommendation and provide additional comments in response to the final report.

Appendix A. Scope and Methodology

We reviewed documentation dated from July 1997 through February 2002. To accomplish the audit objective we:

- Interviewed officials and obtained documentation from the Office of the Army Director of Information Systems for Command, Control, Communications, and Intelligence; the Army Materiel Command; the Army Space and Missile Defense Command; the Program Executive Office Air and Missile Defense; the Program Executive Office Tactical Missiles; and AMCOM.
- Reviewed the AMCOM Distributed Computing Environment Benchmark Study, March 2001.
- Reviewed the cost analysis that addressed combining the Integrated Center Information System and the Automated Resource Management System as a single resource management system in support of AMCOM.
- Analyzed technical direction orders applicable to the AMCOM Information Mission Area Support Services Contract to determine requiring organizations and technical monitors responsible for accepting information technology deliverables totaling more than \$22 million in FY 2001.
- Reviewed eight technical direction orders at a cumulative cost of more than \$1.5 million for information technology services issued between March and November 2001 by the Aviation and Missile Research, Development, and Engineering Center.
- Reviewed the purchase of a \$59,659 training module by the AMCOM Intelligence and Security Directorate.
- Reviewed the \$14,012 purchase card acquisition for a graphics writer by the AMCOM Command Analysis Directorate.
- Reviewed the AMCOM Information Management Master Plan.
- Reviewed Program Budget Decision No. 704 “Financial Management Modernization Program.”
- Reviewed the AMCOM FY 2001 Obligations.
- Analyzed a \$40 million listing of AMCOM FY 2001 credit card transactions to identify information technology purchases.
- Reviewed AMCOM Information System Security processes and procedures.

-
- Evaluated the adequacy of management controls related to the management of information technology at AMCOM.
 - Contacted Department of Army, Army Materiel Command, and officials responsible for the management of information resources and internal management controls at AMCOM. In addition, we contacted persons responsible for the acquisition of information resources at Redstone Arsenal including chief information officers from AMCOM and tenant organizations, contracting officer technical representatives, a contracting officer representative, technical monitors, budget analysts, and other AMCOM personnel who were involved with specific information technology acquisitions.

We conducted this audit from September 2001 through June 2002 in accordance with generally accepted government auditing standards. Except for the Corporate Information Center, AMCOM costs for acquiring, collecting, storing, and reporting information were not readily identifiable because funds were commingled with budgeted costs of other organizations and tenants. Therefore, we relied on discussions with knowledgeable personnel and reviews of contracts for estimating information technology costs.

Use of Computer-Processed Data. We relied on computer-processed data to compare FY 2001 purchase card transactions for information technology to a list of authorized cardholders. Because the scope of our review was limited to identifying information technology transactions, we did not evaluate overall controls for the Purchase Card Management System.

General Accounting Office High-Risk Area. The General Accounting Office has identified several high-risk areas in the DoD. This report provides coverage of the Information Security and Defense Systems Modernization high-risk areas to include Information Management.

Management Control Program Review

DoD Directive 5010.38, "Management Control (MC) Program," August 26, 1996, and DoD Instruction 5010.40, "Management Control (MC) Program Procedures," August 28, 1996, require DoD organizations to implement a comprehensive system of management controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of the controls.

Scope of the Review of the Management Control Program. We reviewed the adequacy of AMCOM management controls for information resources at the Redstone Arsenal. Specifically, we reviewed controls for coordinating and overseeing information management plans and actions made by organizational elements and tenants. Further, we reviewed the self-evaluation applicable to those controls.

Adequacy of the Management Controls. We identified material management control weaknesses as defined by DoD Instruction 5010.40. Controls for information management were not adequate to ensure that applied resources for acquiring information technology products were effectively and efficiently managed in accordance with Office of Management and Budget, DoD, and Army guidance. Implementation of the recommendations to provide information technology training and guidance to technical monitors, to comply with the requirement to engage the CIO in acquisitions of information technology, and to screen purchase card transactions should correct the weaknesses. A copy of the report will be sent to the senior official in charge of management controls for the Army Materiel Command and AMCOM.

Adequacy of Management's Self-Evaluation. AMCOM conducted self-evaluations by organizational element rather than functional area. As a result, when AMCOM performed its self-evaluation of management controls for information resources, the review was limited to the Corporate Information Center and excluded information resources managed and funded by other organizational elements and tenants. Further, when a benchmark study reported that AMCOM had not followed information management and information technology best practices, AMCOM did not consider the study results to be material and chose not to report them to the Army Materiel Command even though information management is a designated DoD high-risk area.

Prior Coverage

During the last 5 years, no reports addressing the Management of Information Resources at AMCOM have been issued.

Appendix B. Mandatory Guidance

Office of Management and Budget Guidance

Office of Management and Budget Circular A-123. Office of Management and Budget Circular A-123, June 21, 1995, defines management controls as the organization, policies, and procedures used to reasonably ensure that:

- programs achieve their intended results;
- resources are used consistent with agency mission;
- programs and resources are protected from waste, fraud, and mismanagement;
- laws and regulations are followed; and
- reliable and timely information is obtained, maintained, reported, and used for decision making.

The Circular explains that management controls guarantee neither the success of agency programs nor the absence of waste, fraud, and mismanagement, but they are a means of managing the risk associated with Federal programs and operations.

Office of Management and Budget Circular A-130. Office of Management and Budget Circular A-130, “Management of Federal Information Resources,” November 28, 2000, implements numerous public laws, including the Clinger-Cohen Act of 1996, that address the acquisition, management, and security of Federal information resources. The Circular defines information resources as both Government information and information technology. It states that CIOs must:

- participate actively in the development, implementation, and maintenance of strategic and operational plans,
- participate actively throughout the budget process in establishing priorities for agency information resources,
- advise the agency head on the design, development, and implementation of information resources,
- monitor and evaluate the performance of information resource investments and advise the agency head on whether to continue, modify, or terminate a program or project, and
- monitor compliance with guidance in the Circular.

In addition, the Circular requires Federal agencies to:

- Develop a well-trained corps of information resource professionals,
- Ensure that improvements to existing information systems and the development of planned information systems do not unnecessarily duplicate information technology capabilities, and
- Ensure that information technology is accessible to individuals with disabilities.

Further, Appendix III requires Federal agencies to establish management controls to ensure adequate security for all information processed, transmitted, or stored in Federal automated information systems and to conduct periodic security reviews to determine the effectiveness of controls.

DoD Guidance

DoD Directive 5010.38. DoD Directive 5010.38, “Management Control (MC) Program,” August 26, 1996, establishes the DoD program for management controls and implements Office of Management and Budget Circular A-123.

DoD Directive 5200.28. DoD Directive 5200.28, “ Security Requirements for Automated Information Systems,” March 21, 1988, implements the security safeguard provisions of Office of Management and Budget Circular A-130.

DoD Instruction 5200.40. DoD Instruction 5200.40, “DoD Information Technology Security Certification and Accreditation Process,” December 30, 1997, implements DoD Directive 5200.28, assigns responsibilities, and prescribes procedures for certification and accreditation of automated information systems, networks, and sites.

Army Guidance

Army Regulation 11-2. Army Regulation 11-2, “Management Control,” August 1, 1994, implements Office of Management and Budget and DoD Guidance for the management control process. It states that all commanders and managers have an inherent responsibility to establish and maintain effective management controls, assess areas of risk, identify and correct weaknesses, keep their superiors informed, and give high priority to weaknesses in identified high-risk areas. The Regulation requires the heads of major Army commands to sign an annual statement of assurance that accurately describes material weaknesses and planned corrective actions. Also, a material control weakness must warrant the attention of the next level of command and a corrected weakness does not preclude it from being reported at the next higher level.

Army Regulation 25-1, Army Information Management. Army Regulation 25-1, “Army Information Management” February 15, 2000, implements Office of Management and Budget and DoD Guidance for the management and security of information resources and information technology as applied to command and control systems, intelligence systems, business systems, and national security systems. The Regulation:

- States that, as a valuable resource, information must be managed as any other asset, such as funds, personnel, and equipment.
- Requires CIOs in Army subordinate organizations to provide management oversight for information technology investments and to serve as the senior information management official.
- Requires that all information systems be subjected to an established certification and accreditation process for verifying that information assurance is achieved and sustained.
- Provides a checklist to evaluate management controls for information management and information technology functions.

Further, the Regulation states that information systems integration throughout an organization generally reaps efficiency dividends among functional areas.

Army Regulation 380-19. Army Regulation 380-19, “Information Systems Security,” February 27, 1998, implements DoD Guidance governing information security. The Regulation requires that system administrators be trained in all aspects of information system security. Further, the Regulation requires that before operation, each automated information system be certified and accredited for security requirements and safeguards, and be approved by the information system security manager (or officer).

AMCOM Guidance

AMCOM Regulation 25-4. AMCOM Regulation 25-4, “Information Management,” June 9, 1999, implements Army guidance for the management and security of information resources applicable to command and control, intelligence, business, and national security systems. The AMCOM Regulation requires CIO approval to purchase information technology products and services and prescribes the process that organizations and tenants must follow to coordinate their information technology purchases with the CIO. In addition, the Regulation requires purchase cardholders to obtain annual Deputy CIO authorization before purchasing information technology products.

Appendix C. Validation of Assertions Made in the Hotline Allegation

An allegation made to the DoD Hotline by an anonymous source asserts that the Army Aviation and Missile Command (AMCOM), located at the Redstone Arsenal, Huntsville, Alabama, had mismanaged information resources. The following discussion summarizes the assertions made in the allegation and addresses their validity.

Assertion 1. AMCOM allowed its Centers, Directorates, and tenants to acquire and manage information technology resources without coordinating actions with the Chief Information Officer (CIO) and the Corporate Information Center.

Response. The assertion was valid. The CIO and the Corporate Information Center did not always review the information technology requirements that AMCOM organizational elements and tenants subsequently acquired.

Assertion 2. AMCOM obtained information technology with untrained personnel.

Response. The assertion was valid. Technical monitors who had no information technology training made quality assessment recommendations for deliverable products received from the Information Mission Area Support Services Contract.

Assertion 3. AMCOM did not empower its CIO to select, control, and oversee command and area-wide information technology investments and operations.

Response. The assertion was not valid. AMCOM Regulation 25-4, "Information Management," June 9, 1999, does empower the CIO. Although it does not specifically state that the CIO manages information resources at the Redstone Arsenal, the Regulation provides procedures that engage the CIO in the Command's areawide information management business processes.

Assertion 4. AMCOM acquired software applications that will be replaced in 2002 when the Army deploys the Wholesale Logistics Modernization Plan.

Response. The assertion was not valid. Business process applications for the Wholesale Logistics Modernization Plan have not been completed, and AMCOM has not reengineered its processes or acquired software that will be replaced when the Army deploys the Plan's applications.

Assertion 5. AMCOM purchased software applications that duplicated similar business processes.

Response. This assertion was partially valid. AMCOM does operate and maintain systems that augment similar functional processes in its organizational elements. In 1998, a joint analysis team determined that an annual \$431,000 cost avoidance would result by combining modules of two resource management information systems.

However, action was delayed pending results from further studies. As of November 2001, documentation could not be found indicating the resumption of additional studies.

Assertion 6. AMCOM did not comply with information security guidance.

Response. The assertion was valid. Acquiring a graphics writer in 1999 with a purchase card, the Command Analysis Directorate connected it to the Redstone Arsenal Campus Network without certifying that it complied with Federal Information Processing and DoD implementing information assurance requirements.

Appendix D. Information Resource Management at Redstone Arsenal

Organization	Extent of System Involvement	Assigned Staff	Types of Services	Information Technology Funds for FY 2001
AMCOM Corporate Information Center	Operates and maintains the AMCOM Campus Area Network	265 information technology professionals Contracted personnel	Operates and maintains the Redstone Arsenal Campus Area Network Develops and sustains functional applications Provides technical support to AMCOM organizations and tenants Maintains worldwide network connections	\$82 million – Actual Costs
AMCOM Acquisition Center	Local area network servers with user access to database programs	22 procurement analysts technicians and clerks Contracted personnel	Network administration	Estimated to be as much as \$350,000
AMCOM Integrated Materiel Management Center	Local Area Network and e-mail servers Application servers to support its business functions 5 servers for the Multi-user Engineering Change Proposal Automated Review System	9 administrative personnel 2 logisticians Contracted personnel	Web software and database applications development New technology system integration and support Help Desk support	Estimated to be as much as \$3 million
AMCOM Research, Development and Engineering Center	Local Area Network and e-mail servers	Division focal points	Network operations Software development	Estimated to be as much as \$2 million
AMCOM Command Analysis Directorate	Connected to the Redstone Arsenal Campus Area Network Connected to a Defense Information Systems Agency mainframe computer	1 information technology specialist Contracted personnel	Network administration Software development	Estimated to be as much as \$73,000
AMCOM Security Assistance Management Directorate	A local area network with 2 servers for accessing DoD and Army mission applications.	6 program specialists 1 logistician 1 management assistant Contracted personnel	Network Administration Help Desk support	Estimated to be as much as \$490,000

Source: Discussions with information technology points of contact within each Organizational Element or Tenant activity

Organization	Extent of System Involvement	Assigned Staff	Types of Services	Information Technology Funds for FY 2001
AMCOM Intelligence and Security Directorate	Redstone Arsenal Campus Area Network. Information assurance focal point for Redstone Arsenal	2 security specialists Contracted personnel	Information assurance	Identified \$60,000
AMCOM Test, Measurement, and Diagnostic Equipment Activity	Local area network with 18 to 20 servers 3 Unix computers to support mission databases Intranet network with worldwide users	8 computer specialists 3 data or information management specialists 1 accounting specialist 1 administrative assistant Contracted personnel	Network administration Intranet hosting Application development	Estimated to be more than \$1.2 million
AMCOM Resource Management Directorate	Local area network and e-mail servers Mission applications on a mainframe computer at the Defense Finance and Accounting Service, St. Louis	1 systems management analyst Contracted personnel	Help Desk support	Identified \$5,250
Program Executive Office for Tactical Missiles and Smart Munitions	An enterprise network linked to: Local area networks individually owned and operated by each program management office The Redstone Arsenal Campus Area Network for worldwide connectivity	13 people in various job series Contracted personnel	Network support System security	Identified \$2.6 million
Program Executive Office for Air and Missile Defense	Wide area network and e-mail, database servers, security intrusion detection devices, and applications Communications services, automated data processing maintenance, and internet received from AMCOM	1 person responsible for information technology Contracted personnel	Network support Intrusion detection Reporting security certifications and accreditation Policies, procedures, and management controls	Estimated to be as much as \$3.5 million.
Army Materiel Command Logistics Support Activity	Local area network 28 servers for mail, database, and management applications	50 computer specialists 6 information specialists 20 additional people in various job series Contracted personnel	Network support Technical support on specific projects	Estimated to be as much as \$27.6 million
Deputy for Systems Acquisition	Redstone Arsenal Campus Area Network Each program office operated and maintained its own hardware Note: The Deputy for Systems Acquisition was disbanded in November 2001	2 persons responsible for information technology Contracted personnel	Staff and technical assistance	Estimated to more than \$2.8 million

Source: Discussions with information technology points of contact within each Organizational Element or Tenant activity

Appendix E. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense (Comptroller)/Chief Financial Officer
Deputy Chief Financial Officer
Deputy Comptroller (Program/Budget)
Assistant Secretary of Defense (Command, Control, Communications and Intelligence)

Department of the Army

Assistant Secretary of the Army (Acquisition, Logistics, and Technology)
Assistant Secretary of the Army (Financial Management and Comptroller)
Inspector General, Department of the Army
Auditor General, Department of the Army
Chief Information Officer, Department of the Army
Commander, Army Materiel Command
Commander, Army Aviation and Missile Command

Department of the Navy

Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Auditor General, Department of the Air Force

Non-Defense Federal Organization

Office of Management and Budget

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations

Senate Subcommittee on Defense, Committee on Appropriations

Senate Committee on Armed Services

Senate Committee on Governmental Affairs

House Committee on Appropriations

House Subcommittee on Defense, Committee on Appropriations

House Committee on Armed Services

House Committee on Government Reform

House Subcommittee on Government Efficiency, Financial Management, and Intergovernmental Relations, Committee on Government Reform

House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform

House Subcommittee on Technology and Procurement Policy, Committee on Government Reform

Department of the Army Comments



DEPARTMENT OF THE ARMY
U.S. ARMY AUDIT AGENCY
OFFICE OF THE DEPUTY AUDITOR GENERAL
ORGANIZATIONAL EFFECTIVENESS
3101 PARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22302-1596

SAAG-PMO-S (36-2c)

29 August 2002

MEMORANDUM FOR Deputy Director, Acquisition Management
Directorate, Office of the Assistant Inspector
General for Auditing of the Department of
Defense, 400 Army Navy Drive, Arlington, VA
22202-2884

SUBJECT: Report on Information Resource Management at the Army
Aviation and Missile Command (Project D2001-AL-0173)

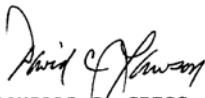
1. References:

a. Draft DODIG Report, 20 June 2002, Information Resource Management at the Army Aviation and Missile Command, Project D2001-AL-0173.

b. U.S. Army Materiel Command memo, 6 August 2002, SUBJECT: DODIG Draft Report, Information Resource Management at the Army Aviation and Missile Command, Project D2001-AL-0173 (AMC No. D0141).

2. Enclosed are the U.S. Army Materiel Command comments on the draft report.

3. If you need assistance, please contact Mr. David Lawson, in my Liaison Branch, at (703) 614-9425, fax 614-9461, or e-mail lawsond@aaa.army.mil.


DONALD C. CRESS
Deputy Program Director
Organizational Effectiveness



DEPARTMENT OF THE ARMY
HEADQUARTERS, U.S. ARMY MATERIEL COMMAND
5001 EISENHOWER AVENUE, ALEXANDRIA, VA 22333 - 0001

REPLY TO
ATTENTION OF

AMCIR-A (36-2A)

6 Aug 02

MEMORANDUM FOR MR. DONALD C. CRESS, PROGRAM DIRECTOR, STRATEGIC
ENGAGEMENT OFFICE, U.S. ARMY AUDIT AGENCY, 3101 PARK CENTER DRIVE,
ALEXANDRIA VA 22302-1596

SUBJECT: DODIG Draft Report, Information Resource Management at the Army Aviation and
Missile Command, Project D2001-AL-0173 (AMC No. D0140)

1. We are enclosing our position on subject report IAW AR 36-2.
2. We concur with the AMCOM comments. While we consider the report's finding and recommendations to be generally true throughout the DoD and across many government agencies, we believe the new Army Knowledge Management (AKM) directives, once fully implemented, will seek to resolve the issues in this report.
3. Point of contact for this action is Ms. Jennifer R. Baxter, (703) 617-0530, e-mail -baxterj@hqamc.army.mil.

FOR THE COMMANDER:

Encl
as

For the P. Hack loc 65
RICHARD A. HACK
Major General, USA
Chief of Staff
Dep Chief of Staff

COMMAND COMMENTS
DODIG Draft Report
"Information Resource Management at the
Army Aviation and Missile Command"
(DODIG Project D2001AL-0173)
(AMC Project D0140)
(AMCOM Project 03-0801-053)

Additional Facts: It should be noted that the Army is currently going through and is planning for a major reorganization. Consequently, significant changes are occurring in the way that information technology (IT) is managed throughout the Army. Specifically, under the Army's Transformation in Installation Management (TIM) concept, effective 1 October 2002, an installation, Director of Information Management (DOIM) will be established under a new garrison organization to serve as the single installation DOIM for Redstone Arsenal. Under this concept, the installation DOIM will be responsible for, approving IT requirements for the Army Aviation and Missile Command (AMCOM) and those of other Army tenants. As a result, AMCOM will submit its IT requirements—development of mission applications and data management remains the responsibility of the mission commander under the TIM concept --to the DOIM for approval, acquisition of hardware and software, and provision of services. As a result, some of the recommendations in the report may not be the responsibility of AMCOM in the future.

Recommendation 1:

We recommend that the Commanding General, Army Aviation and Missile Command provide technical monitors with training and guidance in the basic information technology concepts necessary to evaluate the acceptability of products and services obtained from the Information Mission Areas Support Services Contract.

Action Taken: Partial Concur. The Corporate Information Center will establish an Information Technology course of instruction to ensure technical monitors have a standard level of knowledge for evaluating the quality of deliverable services received on the Information Technology Support Services contract. The course of instruction will be designed to provide technical monitors with a fundamental knowledge of Information Technology disciplines. We anticipate implementing the training within three to six months.

As an additional control, the Corporate Information Center implemented a network design review for new network equipment being added to the AMCOM infrastructure. The review is performed by the CIC network staff and should help ensure consistency in the product provided by the contractor workforce.

Recommendation 2: We recommend that the Commanding General, Army Aviation and Missile Command establish controls to ensure that the Army Aviation and Missile Command and tenant organizations engage the Chief Information Officer in business system acquisitions of information technology in accordance with Army Aviation and Missile Command Regulation 25-4, "Information Management."

Action Taken: Concur with the intent of the recommendation. Although a control process was already in place to oversee IT purchases, AMCOM strengthened its controls by completing the development of a comprehensive Information Management Master Plan (IMMP) on 3 April 2002. The IMMP includes controls for the Business Information Management Planning Board (BIMPB), chaired by the AMCOM Chief Information Officer (CIO), to perform a structured review of IT initiatives, regardless of funding source, to ensure compliance with statutory and regulatory guidance and to validate the link between IT expenditures and the AMCOM mission. It also requires the BIMPB to review and prioritize initiatives and submit them to the AMCOM Board of Directors (BOD) for approval, before submission through funding channels. (Tenant organizations have the option of their higher headquarters delegating approval authority to the CIO for IT initiatives, or going through their own command channels for IT approvals.)

Recommendation 3: We recommend that the Commanding General, Army Aviation and Missile Command screen purchase card transactions to ensure that information technology products and services are acquired by approved cardholders.

Action Taken: Concur with the intent of the recommendation. Controls in the AMCOM Information Management Master Plan (IMMP) cover the acquisition of IT supplies and services regardless of the means used to purchase them (e.g. purchase cards or conventional purchases). Specifically, the IMMP requires the Business Information Management Planning Board (BIMPB) to review and prioritize initiatives and submit them to the AMCOM Board of Directors (BOD). Membership on the BIMPB includes a representative from each AMCOM organization, and BOD membership consists of the Primary Organizational Element (POE) for each AMCOM organization. In addition to controls established in the IMMP, AMCOM also developed or already had developed other controls for acquiring IT products and services:

- The Corporate Information Center (CIC) web site contains supporting guidance for purchasing IT resources, including a list of approved IT resources that C&I only be purchased with a purchase card.
- The Chief Information Officer (CIO) has a CIC representative who explains the guidance and procedures associated with IT credit card purchases during credit card holder training.
- The CIO/CIC is the proponent of an AMCOM regulation, which provides credit card holders involved in

purchasing IT resources with applicable responsibilities and procedures.

- The Acquisition Center's "Government Purchase Card Internal Operating Procedures (IOP)", dated 3 April 2002, contains guidance for billing officials to use for making sure that cardholders' purchases are allowable and that IT approvals have been obtained.

Also, the CIO/CIC has begun developing a web-based automated system for the submission, review, and approval of AMCOM IT requirements. Plans are for the system to have the capability to capture IT expenditures by individual organizations, and to identify a specific credit card holder within an organization.

Recommendation 4: We recommend that the Commanding General, Army Aviation and Missile Command reassess the identified annual cost avoidance opportunity of combining the Automated Resource Management System and Integrated Center Information System modules.

Action Taken: Nonconcur. A command Integrated Process Team (IPT) consisting of senior analysts from the AMCOM Corporate Information Center, Resource Management Directorate, and Research, Development, and Engineering Center (AMRDEC), which was in force from January –September 1998, determined that the cost avoidance of \$431,000 had been improperly calculated. This was because it included the cost of eleven scientific processing employees who had no relationship to Integrated Center Information System (ICIS). By September 1998, the IPT had reached a consensus that since MRDEC is the only AMCOM organization that requires the level of detail provided by ICIS, it was not feasible; and would not be cost effective, to merge ICIS and Automated Resource Management System (ARMS). As a result, the methodology and rationale for developing the cost savings is questionable.

Recommendation 5: We recommend that the Commanding General, Army Aviation and Missile Command report the actions taken to correct weaknesses in information management and information technology best practices contained the "U.S. Army Aviation and Missile Command Distributed Computing Environment (DCE) Benchmark Study" in the Aviation and Missile Command, FY 2002 Statement of Assurance and subsequent statements until actions are completed.

Action Taken: Concur with the intent of the recommendation. The AMCOM CIC established an IT Working Integrated Process Team (WIPT) composed of members from each AMCOM major organizational element. The WIPT is analyzing the recommendations made in the Harris study (which addresses business processes only) to develop a business case analysis (BCA) for each of the recommendations by using the following methodology:

- Document the existing method used at this command for the item under study (the as-is model).
- Develop methods of performing alternatives to the as-is model, based on the recommendations from the Harris study and listed in the charter.
- Determine the advantages or disadvantages of each alternative in the study.
- Determine the costs associated with each method.
- Make recommendation to the AMCOM Board of Directors (BOD) concerning selection.

As a result of the analysis, the BCA process is about 70 percent complete with several recommendations already approved for implementation, pending funding. Until the IPT determines the validity of the study, we will not assume that we have material weaknesses in this area. We will continue to review existing IT processes for material weakness and possible improvements. As material weaknesses occur, that we cannot readily correct and should report, we will identify and report them through proper channels.

Recommendation 6: We recommend that the Commanding General, Army Aviation and Missile Command evaluate all Redstone Arsenal information management and information technology functions and report any material weakness in the Army Aviation and Missile Command FY 2002 Statement of Assurance.

Action Taken: Concur with the intent of the recommendation. The AMCOM CIO has implemented and/or improved many information management business processes to allow better management controls and accountability of IT resources. We will continue to review existing IT processes for material weakness and possible improvements. As material weaknesses occur, that we cannot readily correct and should report, we will identify and report them through proper channels.

Team Members

The Acquisition Management Directorate, Office of the Assistant Inspector for Auditing of the Department of Defense prepared this report. Personnel of the Office of the Inspector General of the Department of Defense who contributed to the report are listed below.

Mary L. Ugone
Charles M. Santoni
David M. Wyte
Stephen J. Bressi
Robert R. Johnson
Leann A. Alwood
John R. Huddleston
Jacqueline N. Pugh